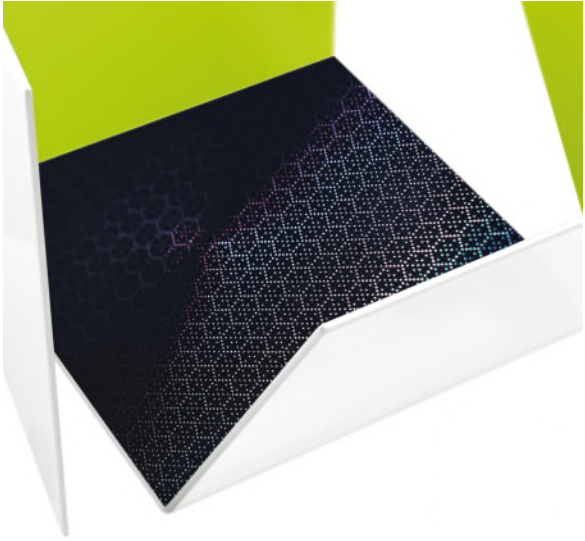
Hogan Lovells



# AI & Data Regulation: What privacy professionals need to know about the EU, UK, and U.S. approaches

Spring 2023

## Current Legislative and Regulatory Landscape

1. **Current AI proposals in the EU**
   - AI Regulation
     - Goal: The Regulation aims to address risks created by AI and to position the EU as the lead from a legal perspective. It focuses on trustworthiness of AI and the impact on individuals, society, and the economy.
     - It is a Regulation, so once it comes into force, it will apply throughout the EU without further implementation at local levels (member states). This is similar to the GDPR.
     - Status: It has been approved by EU Commission and Council and is now subject to approval by EU Parliament, which is expected April 2023, and the rules could apply to organizations by as early as mid-2025.
   - AI Liability Directive
     - Goal: The Directive aims to ensure individuals who suffered damages can claim violations of civil law.
     - It is a Directive, so once adopted, it will need to be implemented and harmonized on a local level with each individual EU member state.
     - Status: The Directive has yet to be debated by the EU Council and Parliament.
   - EU Position on AI: The EU is looking to be the leader with respect to how AI will be regulated (in the same way they did with the GDPR). The goal is for these AI principles to be used globally.
2. **Current AI Proposals in the UK**
   - There is currently no AI specific law in the UK, but there are privacy, anti-discrimination, and consumer protection requirements which currently apply.
   - In July 2022, the UK government published a white paper blueprint for an AI specific regulation, which has since been updated through a more detailed proposal in March 2023.
     - The UK government's position is diametrically opposed to what the EU is trying to achieve with AI Act. (*This discrepancy raises a critical question about how best to regulate and how to reach a global standard for compliance with AI.*)
       - The EU focuses on rights of individuals, and the UK is more business friendly.
       - The EU prescribes product liability-style regulations, and the UK has more principle-based requirements.
       - The EU takes a cross-sector approach, and the UK is looking to existing regulators to interpret the core principles as a basis for practical guidance in specific sectors and domains.
3. **Contrasting the EU and UK approach to the current approach in the US**
   - Similar to the landscape with privacy, the U.S. does not have comprehensive AI legislation. Instead, federal, state, and local governments have progressed with sector- or use-case specific regulation. It is not feasible to cover all of the proposals across the U.S. However, some of the notable developments for AI regulation in the U.S. are outlined below.
   - The United States Government has adopted a whole-of-government approach to regulating AI. These efforts are proceeding primarily through existing regulatory authority or voluntary initiatives.

- Many of the federal actions are intended to advance the White House's AI Bill of Rights ("AI Bill of Rights").
  - The AI Bill of Rights has five principles for AI systems that have the potential to impact civil rights of Americans: (i) safe and effective systems, (ii) algorithmic discrimination protections, (iii) data privacy, (iv) notice and explanation, and (v) human alternatives.
  - The AI Bill of Rights is non-binding, so it doesn't have the force of law. But the White House did direct all Executive agencies to look for a way to promote the principles of the Bill of Rights.
- The Federal Trade Commission has released several guidance documents relating to AI in recent years. The guidance makes clear the FTC is concerned about bias, misrepresentation, lack of accountability measures, and misuse.
  - Chatbots, deepfakes, and voice clones: AI deception for sale | Federal Trade Commission (Mar. 20, 2023)
  - Keep your AI claims in check | Federal Trade Commission (Feb. 27, 2023)
  - Aiming for truth, fairness, and equity in your company's use of AI | Federal Trade Commission (April 19, 2021)
  - Using Artificial Intelligence and Algorithms | Federal Trade Commission (April 8, 2020)
- The Equal Employment Opportunity Commission has an AI and Algorithmic Fairness Initiative and has released guidance exploring how the Americans with Disabilities Act applies to AI-supported hiring.
- The Department of Health and Human Services recently proposed regulations reinterpreting section 1557 of the Affordable Care Act to prohibit discrimination by clinical algorithms, among other changes.
- The Department of Housing and Urban Development and Department of Justice recently submitted a statement of interest in pending litigation on the issue of tenant screening algorithms and the Fair Housing Act.
- The White House's AI Bill of Rights Fact Sheet identified additional initiatives across the executive branch to implement the AI Bill of Rights, including updates to procurement rules.
- The American Data Privacy and Protection Act ("ADPPA"), which was introduced last year, included provisions on algorithms and impact assessments.

- States and even municipalities are looking to regulate AI, with some of these requirements having already passed. As above, these requirements are typically sector- or use case-specific.
  - In the employment context:
    - New York City Local Law 144 imposes new requirements on the use of automated employment decision tools, including the requirement to undertake annual bias audits. (More on Local Law 144's implementing regulations can be found here). Similar laws are being considered in California, New Jersey, New York, and potentially other states.
    - Other laws in this space include Illinois's AI Video Interview Act and Maryland's law regulating use of facial recognition in interviews.
    - California's state agencies are also actively regulating in this space: the California Civil Rights Department is considering proposed regulations on automated decision systems and the California Privacy Protection Agency is soliciting comments in advance of a rulemaking on under the California Consumer Privacy Act.
  - Colorado's Division of Insurance has released proposed regulations requiring AI governance for algorithms and predictive models.
  - The Massachusetts Gaming Commission has released privacy, security, and automated decision-making regulations for gaming licensees and sports wagering operators. Our summary of these regulations can be viewed here.
  - Many of the state consumer privacy laws allow consumers to opt out of profiling in furtherance of decisions with legal or similarly significant effects.

## Common Core Components of Proposed Legal Approach to Regulate AI

1. **Data governance**
   - AI Regulation: For high-risk AI systems to be used there are a range of technical and organizational requirements that have to be implemented by providers, including a risk assessment and a conformity assessment on a regular basis (making sure what an AI systems work in accordance with the Act's requirements).
   - AI Act: The AI Act expects organizations to have an AI governance system in place and in practice will require close collaboration between people with a technical and legal risk background that can do the following:
     - Implement technical measures during the design, development and deployment of AI;
     - Create policies and procedures regarding the use of AI;
     - Train individuals within the company on the organization's use of AI and the organization's AI strategies (in parallel with some supervision of the use of AI); and
     - Monitor how AI is operating in a live production environment and how the potential impact of the AI can be explained to an individual.
   - An organization can only do all these things if they have a good inventory of the AI systems used within your organization. Now organizations can start taking an inventory but asking answering the following questions:
     - What do we use?
     - How do we use it?
     - What is the potential impact to the individual?
     - How do we bring that in line with the proposed AI regulation?
   - Organizations can learn a lot from what has been developed for the GDPR from a governance perspective, and this can be re-used. Organizations can re-use existing policies and procedures, and governance structures can help companies drive towards AI compliance.
   - What is the overlap between these proposals and existing data protection laws? How can a data protection program address data protection and future AI regulation?
     - Organizations should make sure they have data governance and make sure how they are using data is in accordance with expectations.
     - Organization have to make sure data is accurate, necessary, and is secure (and perform an impact assessment of the risk of using that data).
     - These are all elements we know from a data protection perspective, so now that is being extended to AI systems – data minimization, accuracy, security, transparency – which is familiar to a lot of companies.
2. **Ethics and algorithmic bias**
   - What we are now seeing is through the legislative initiatives is principles being placed on a "satisfactory" footing. For example, the AI Act does not require AI systems to be unbiased perse. Instead requirement is not to be unbiased entirely because that would be unfeasible.
   - Instead, the regulation focuses on the practical means to rectify harmful biases (e.g., unlawful discrimination). Those practical means include data governance, risk assessment, and monitoring AI systems in the live production environment.
   - What organizations should be doing:
     - Identify risks posed by certain AI systems.
     - Seek to deploy practical interventions on the use of the AI system to mitigate risk.
3. **Risk management**
   - Risk assessments and management are critical components to forthcoming AI regulatory structures in the EU, UK, and U.S., and are often the starting point for discussions around AI regulation.
   - The EU AI Act's regulatory structure centers on risk tiers relating to the AI applications in question, as described above. Similarly, in the UK, the government has proposed a risk-based approach, focused on identifying and managing risks associated with AI. (Our summary of the UK's proposal is here).
   - In the U.S., risk considerations may not be expressly stated but are often implicit in the regulatory structure. Sector- or use case-specific AI regulations arise in scenarios deemed to be higher risk.

- For example, consumer privacy laws in Virginia, Colorado, and Connecticut allow users to opt out of profiling in furtherance of decisions with legal or similarly significant effects.
- Relatedly, California AB 331, a pending piece of legislation that would regulate "automated decision tools" involved in making decisions in more sensitive contexts such as employment, education, housing, healthcare, financial services, criminal justice, and legal services.
- The AI Bill of Rights similarly incorporates a risk dimension by limiting its (voluntary) application to automated systems that "have the potential to meaningfully impact rights, opportunities, or access to critical resources or services."
- Some U.S. regulations expressly require risk assessments and management however, such as Colorado's proposed AI governance regulations for the insurance industry. In addition, the U.S., through the National Institute of Standards and Technology, has also released a voluntary Artificial Intelligence Risk Management Framework that provides seven traits of trustworthy AI and describes the components of a risk management framework that can be adapted by various actors across the ecosystem. Our summary of the AI RMF and associated resources is here.

- The steps organizations take to management AI-related risks will also be relevant to regulatory enforcement under unfairness consumer protection authorities and to determine whether a company has met its standard of care in civil litigation (including product liability claims).

4. **Accountability**
   - Accountability is all about being able to demonstrate that an organization is making the right decisions and that they thought in advance before implementing AI systems.
   - Organizations should use DPIAs as a basis to consider AI compliance, to assess risk and, and to implement measures to mitigate AI risk.
   - Accountability will be very useful in making a determination in an organization's global AI strategy.
5. **Transparency**
   - Transparency is an important part of accountability and vice versa. Regulations are frequently looking at transparency as a key element of AI governance.
   - We see at least three types of transparency:
     - Transparency on the intended uses and limitations of the model (what the AI is and what it is not intended to do).
     - Transparency about the model design and data practices (incl. training data) (how was the model made and trained).
     - Transparency about a particular output or decision, both in terms of explaining the reasons for a decision and in notifying end users when automated decisions are being made.
6. **Human oversight**
   - AI is designed to help humans and humans will need to provide oversight.
   - Accountability requires:
     - working with organizational elements; and
     - working hand-in hand with engineers to make sure AI by design is being implemented at a practical level
   - There are two types of human oversight:
     - Active: Active oversight involves human intervention on an individual decision level which may take place due to the context the AI system is being used (e.g. health care system being able to predict the outcome of cancer screenings which you would want a medical professional to agree and verify).
       - An example of active monitoring measures in the active environment could be identifying excessive numbers of false positives in the outputs, or identifying disparities of treatment of minority groups.
     - Passive: Passive oversight looks at the overall performance of a system and takes a holistic level view.
7. **Safety and security**
   - Regulators are also increasingly concerned about the safety of AI applications, which is related to ethics and bias but goes beyond that to include considerations around emergent behaviors.

## How to Prepare for the Inevitable Regulation on the Development and Use of AI

- **Assess current uses/plans for AI development and use:** Organizations should take stock of their use and development of AI systems and consider the following (in order):
    1. The first step organizations should take is assess the potential impact of these various regulations that have been discussed above and how they apply to your organization now. Laws are being developed, but we have a clear understanding of the extent the AI Act is going to be applicable and the types of rules that are going to be in place. The rules and regulations may evolve, but this is a useful starting point.
    2. What is your role as an organization?
        - The AI Act creates different roles for AI systems – general purpose AI systems, high-risk AI systems, and users of AI systems (those deploying AI systems).
    3. Whether the laws have an extraterritorial effect.
- What is an AI system?
    - Each jurisdiction may come to a different conclusion here.
    - Something that is really critical that distinguishes AI from a standard software application is the degree of autonomy that is involved. Software applications typically are deterministic – there is a clear path and with AI there isn't a clear path and that is the whole point is to allow you to generate outputs based on environments which haven't been previously seen. So that degree of autonomy is something that should be considered.
    - Should be prepare that the definition of AI could be broad.
- **Impact/risk assessments**
    - What kind of risk assessments are expected? Is the purpose just to identify the risks? How are those risks expected to be addressed? Compare against existing DPIAs under GDPR -- who does them, how do they need to be documented, when do they need to be reviewed.
        - DPIAs would look similar for AI systems:
            - There is a lot we already know and one of that is assessing the risk and mitigating risks and using a DPIA in this regard.
            - If you document the DPIA in the right way you can use this to explain to regulators, the market, and individuals of how the system looks and how it complies with the laws and rules that are applicable to you. Organizations should use the DPIA as a starting point.
    - What is unique about how to conduct risk assessments under US laws?
        - As mentioned above, risk management is implied in many of the U.S.-based regulations. Explicit risk assessment requirements also exist depending on the sector and states in which you do business and the intended use of the AI application. For example, organizations that use automated systems in support of decisions with legal or similarly significant effects may need to prepare documented privacy impact assessments under state consumer privacy laws.
        - Aside from the express regulatory requirements, risk assessments are also important ways to manage legal and reputational risks, such as:
            - Consumer protection claims (e.g., unfair and deceptive)
            - Civil claims (e.g., negligence / product liability claims)
            - Other concerns (e.g., putting in place controls to manage unchecked reliance on generative AI outputs)
- **Policy Development:** How would you think about the issue of organizations using AI / purchasing from a third party? In other words, organizations using AI systems that they didn't develop themselves (e.g., ChatGPT).
    - As a user you need to think about it from two perspectives:
        1. What are the things you can control internally?
        2. What governance measures can you put in place? (e.g., conducting due diligence at the beginning of an engagement, assess an AI tool to determine if it works to a degree of accuracy and is considered appropriate for the use case you are intending to deploy it for, and ongoing monitoring of AI human oversight.)

- Organizations need to be able to envisage the AI systems will change in how it operates over time. A model that works perfectly when you go live may be different 12 months down the line.
- Organizations can also integrate contractual measures (e.g., AI specific terms into contracts).

## Summary

- There is a lot happening with AI right now. It is complicated, but when you look through all the noise you will see these key 7 core components present over and over again.
  1. **Data Governance**
  2. **Ethics and algorithmic bias**
  3. **Risk management**
  4. **Accountability**
  5. **Transparency**
  6. **Human oversight**
  7. **Safety and security**
- Prepare now: If we know the 7 core components above, we are not unprepared to go take the next step around the development and use of AI today by trying to take those core components and integrate them in how we use AI even if they are not legally required to do today. Organizations who did this in advance of the GDPR were much better prepared to deal with the significant movement and requirements that happened with data protection when the GDPR was released. Organizations who complied with GDPR were much better capable of dealing with the requirements in California, in China, in Brazil, and all of the global developments.
- Act now: Those core 7 components and there, and there are specific actions you can take as discussed above.

## Key Contacts


**Scott Loughlin**
Partner | Washington, D.C.
scott.loughlin@hoganlovells.com
+1 202 637 5565

**Joke Bodewits**
Partner | Amsterdam
joke.bodewits@hoganlovells.com
+31 20 553 3645

**Dan Whitehead**
Counsel | London
dan.whitehead@hoganlovells.com
+44 20 7296 2052

**Filippo A. Raso**
Senior Associate | Washington, D.C.
filippo.raso@hoganlovells.com
+1 202 637 6537