CIPL AT 20 — SHAPING DATA POLICY FOR TOMORROW
HUNTON ANDREWS KURTH

29 July 2021

CIPL Response to the EU Commission's Consultation on the Draft AI Act

CIPL[1] welcomes the Consultation on the European Commission's Proposal for a European Artificial Intelligence Act[2] (the "AI Act" or the "Act") to feed into the EU legislative process. CIPL is pleased to see that the AI Act incorporates several recommendations made in CIPL's paper on Adopting a Risk-Based Approach to Regulating AI in the EU.[3] These recommendations are designed to foster trust in AI without hindering its responsible development. In particular, CIPL welcomes the Act's risk-based approach that would apply to high-risk AI use cases while not regulating the AI technology itself or entire sectors. CIPL also welcomes the proposed use of harmonised standards and industry self-assessment of product conformity, as these mechanisms have proven successful in driving innovation and developing safe and trusted technologies in the EU market. CIPL also welcomes the measures designed to support innovation, in particular by providing a statutory basis for regulatory sandboxes. Finally, CIPL is pleased to see that some of the requirements outlined in the AI Act align with some existing industry practices, which set a high bar to ensure that AI is developed and used responsibly.[4]

CIPL regrets, however, that the AI Act does not sufficiently account for imperatives such as providing for outcome-based rules; clearly enabling organisations to calibrate compliance with the requirements based on risks and benefits of the AI system; rewarding and encouraging responsible AI practices; leveraging takeaways from regulatory sandboxes; and clarifying that the AI Act's oversight and enforcement provisions should also be risk-based.

CIPL reiterates that for the AI Act to be effective in protecting fundamental rights while also laying a foundation for a new era in EU innovation, it needs to be flexible enough to adapt to future technologies. Further, the Act must not be overly restrictive so as to avoid suppressing valuable and beneficial innovations and uses of AI across a range of industries and sectors including public health or environment. Finally, the AI Act would benefit from targeted adjustments to better clarify the balance of responsibilities of AI providers, deployers and users, particularly for general purpose AI and open source AI models.

---

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 80 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM/2021/206 final.

[3] CIPL Recommendations on Adopting a Risk-Based Approach to Regulating AI in the EU March 22, 2021.

[4] For example of current industry practices, see note 3, Appendix 3, page 12.

1. Prohibited AI practices

- **Broad definition** - Article 5 of the AI Act identifies several prohibited AI systems. This prohibition relies on concepts such as "subliminal techniques," "beyond a person's consciousness," "materially distort a person's behavior," "likely to cause psychological harm." These terms are new, open-ended and undefined under EU law. If given a broad interpretation, they could inadvertently apply to a wide range of operations that were not intended to be covered by the Act and that are already (or will be) covered by other legislation (such as marketing or advertising activities for instance). These terms would need to be more narrowly defined to provide legal certainty and ensure that only harmful uses of AI are prohibited and that the regulation does not prohibit a variety of other, less risky beneficial uses of AI. The penalties and reputational damage for bringing a prohibited AI system to market may be so significant, that ambiguity in the definition of those practices could have a chilling effect on many potentially beneficial uses of AI.

- **Treatment of research:** The Act should clarify that the publication of pure research that touches upon prohibited (e.g. subliminal manipulation) or high-risk AI systems (e.g. deepfake detection, medical applications, emotion detection) is permitted without restriction and does not qualify as "placing on the market" or "putting into service."

2. Definitions

- **AI** - Article 3(1) of the AI Act relies on an unnecessarily broad definition of "AI." The list of techniques covered in Annex I would capture a significant number of modern software-based products, including a wide variety of systems that are not truly AI applications. Although it is important to use a flexible definition that can adapt to new technologies over time, this language may negatively impact innovation by including many kinds of technologies that only pose trivial or low risks. The definition of AI should be narrowed to apply only to systems that can learn by themselves, adapt over time, generate output and make decisions based on that learning similar to human-level cognitive acts (such as driving a car or making judgments about someone's job application). These kind of systems pose unique risks to fundamental rights and existing legislative frameworks are unlikely to address them. Other systems are already addressed through the GDPR or other regulations that are sufficient to protect individuals in most circumstances. The AI Act should take this into account and expressly exclude human defined systems and processes from its scope.

- **Provider** - Article 3(2) of the AI Act uses an overly broad definition of "provider." This broad definition risks placing undifferentiated burdens on the diverse range of stakeholders that participate in the AI development ecosystem, making it harder to support a healthy ecosystem of innovators, experimenters, contributors, and entrepreneurs. Many different kinds of organisations participate in the AI value chain. Although every organisation has a role to play in ensuring the responsible development of AI, not every organisation can or should shoulder the same obligations.

- **Safety component** –– The notion and scope of safety component in Article 3(14) should be better explained. In particular, it should be clarified whether it is intended (or not) to include cyber security systems.

- **Emotion recognition system** – Organisations would benefit from having concrete use cases that illustrate what type of AI uses are covered by "emotion recognition system" as well as the types of "intentions" that Article 3(34) of the Act aims to capture in this definition.

- **Serious incident** –There is a concern that the concept of "serious incident" in Article 3(44) is defined too broadly as any "incident that […] indirectly leads, might have led or might lead" to certain undesirable events. Liability requires a reasonable standard of causation where the product's defect must be the (reasonably likely) legal cause of the harmful result. Where the causality threshold is weakened, it may allow for excessive responsibilities that contradict the chain of causation. The definition of serious incident should be brought in line with the standard of product liability. There is also a concern that the definition of serious incident as a "serious and irreversible disruption of the management and operation of critical infrastructure" is not aligned with the draft NIS 2 Directive, and could create another layer of "incidents" connected to critical infrastructure for which incident reporting is required.

3. High-Risk AI

- **Broad definition** - Some of the areas and use cases classified as high-risk applications in Annex III seem very broad and could capture AI uses that may not be high-risk at all, conflict with existing law, and have a chilling effect on technologies that have a positive impact on the areas listed in Annex III. For instance, task allocation is considered high-risk under employment-related processes. However, the effects of common task allocation operations do not create the same level of risk as those in, for instance, the recruitment field. Limiting the most onerous regulatory burdens to a narrow list of high-risk AI systems would better enable and support innovation in lower-risk AI applications.

- **AI integrated in consumer devices** - The AI Act qualifies certain systems that are already subject to conformity assessments under specified EU regulations as high-risk AI, such as the Directive on wireless radio equipment. The Act should be clarified to ensure innovation in consumer devices that may use both wireless radio equipment (e.g., Wi-Fi and Bluetooth) and AI, in cases where the AI is not related to the safety of the radio equipment. The AI Act should more clearly distinguish between AI systems that are directly related to, or are integral parts of, the radio equipment subject to regulation, and AI systems that are unrelated to the radio equipment but exist in the same product. Without that distinction, nearly all AI systems used in consumer devices would be considered high-risk AI systems.

- **General purpose AI** - It not clear how and if the rules apply to general purpose AI, where the provider cannot know in advance if the use will ultimately fall under the category of high-risk AI while having no control over how exactly the system will be used. As drafted, the AI Act does not distinguish between

the responsibilities of AI users when acting in a deployer role and the responsibilities of providers to their customers. In such situations, CIPL would recommend that deployers bear the primary responsibility for compliance, as only they know if any additional data has been input into the system and can verify the end-uses of the systems. Providers of general purpose AI systems could, of course, provide all information necessary for the deployer to comply with their obligations, but should not be responsible for something over which they have no control and little-to-no visibility.

- **Open source systems** – It is equally challenging for companies providing open source systems that are not specifically intended for high-risk AI systems, but are nevertheless subsequently used in a manner that could be considered high-risk AI.[5] Such would be the case with an open deep fake detection API that is used by law enforcement authorities, or with traffic routing models used by municipalities to dispatch first responders. As currently drafted, the AI Act would apply to any contributor to the code of an open source AI system. CIPL would recommend that compliance obligations lie with the organisations controlling the purpose and use of the AI system. Imposing obligations on providers of open source systems would disincentivise making the tools available, which would hinder innovation.

- **Amendments to Annex III** - The fact that the EU Commission might change the list in Annex III annually may lead to legal uncertainty. CIPL recommends that industry be consulted throughout the process especially as some concepts on the list, such as "essential services," are broad and vague. As it stands, Article 7 is not fully transparent about the steps and timeline of this decision-making process, despite having substantial impact on AI providers and users who may be affected by future decision-making. Specifically, in relation to Article 7(2) covering the criteria that the Commission shall take into account when assessing whether an AI system poses a risk of harm to the health and safety of individuals, or a risk of adverse impact on fundamental rights, CIPL underlines that:

    - Reports and documented allegations (point c) cannot serve as a legitimate means to demonstrate harms caused by AI systems as they are not transparent and may not comply with due process. CIPL believes that a final decision by a competent court or administrative body, including regulatory agencies, would be a more appropriate standard, provided that the AI system provider/user has had the opportunity to present a full defense and challenge the allegations before a final decision is delivered;

    - The opt-out exception (point e) should be clarified, including by providing examples of opt-out forms which it considers valid;

    - The age element of harm/impact (point f) should be characterised with respect to AI systems that are intended to be used by children, so that this requirement is not extended to the point that it applies to any AI system that may be accessed by a child - which is something materially out of reach for an AI provider/user;

[5] See for instance Tensor Flow https://www.tensorflow.org/

- The element on output reversibility (point g) should be reconsidered in light of the fact that the right to erasure under the GDPR may serve as a mechanism that allows individuals to reverse the outcome produced by the AI system; and

- Regarding impact on data protection rights (point h), the remedies provided for by the GDPR should be regarded as effective measures of redress, including the possibility to lodge a complaint with a data protection authority (DPA).

4. Remote biometric identification

- **Definition** - The definitions of biometric identification are not sufficiently clear in the AI Act. In particular, it is unclear whether some biometric AI systems would not be considered high-risk biometric identification systems. Because the risks and opportunities are so great, it is important to provide clarity. For instance, AI technologies can have significant innovative and positive impacts such as improving healthcare delivery and outcomes, monitoring health and safety, enabling people with disabilities to better navigate the physical world, or could be used for safety and security purposes. The use of biometric data for such purposes, however, is currently a concern within the proposed AI Act.

- **Biometric authentication –** The Act should specifically distinguish biometric authentication from biometric identification, and confirm that biometric authentication falls outside of the scope of the AI Act.6 Biometric identification requires comparing an individual's biometric data to the biometric data of many other individuals stored in a database to identify said individual (i.e. one-to-many matching). On the other hand, biometric authentication entails less risk, given that it consists of comparing two biometric templates usually assumed to belong to the same individual (i.e. one-to-one matching) and no link with the actual identity is established. Biometric authentication is highly beneficial and is often relied upon to ensure verified access to personal data or confidential information.

- **ID verification and ADM** - CIPL underlines that remote biometric identification should not automatically be qualified as "high-risk AI." This would avoid capturing uses such as TouchID on phones, fingerprint access to an office, or online ID verification as part of setting up a bank account. While the underlying ID verification technology could carry risks if it has not been developed fairly, in most scenarios, there will always be a fallback option if the biometric identification fails. The risks would be high only where the failure of biometric ID verification would lead to a significant negative impact on the individual or where there is no fallback option. At the same time, ID verification falls under the definition of automated decision-making under Article 22 of the GDPR and, as such, is

[6] This is consistent with the Commission's February 2020 AI White Paper (in footnote 52), which specified that "remote biometric identification should be distinguished from biometric authentication (the latter is a security process that relies on the unique biological characteristics of an individual to verify that he/she is who he/she says he/she is)."

already subject to specific safeguards where decisions may produce a legal effect or similarly significant effects on individuals. At this stage, it is not clear what the AI Act would add to the GDPR and there a risk of overlap or conflict with the existing GDPR provisions.

- **Consent to biometric identification -** CIPL understands the high-risk qualification of "remote biometric identification" aims to cover situations where biometric data is used to identify individuals without their knowledge, rather than a situation where a well-informed individual deliberately chooses to confirm or reveal his/her identity to transact or otherwise interact with a service provider under certain circumstances, such as an e-commerce platform, in-person shop or an online government service based on his/her biometrics. The Act provides that a system is a biometric identification system if it operates in an indiscriminate manner, i.e., "without prior knowledge of the user of the AI system whether the person will be present and can be identified." Based on this language, it is not clear the extent to which users can consent to the use of biometric identification systems, what kind of consent would be sufficient, and whose consent would be necessary. The answers to these questions should be carefully calibrated to not foreclose beneficial uses of AI to which people would be willing to consent if given the appropriate opportunity.

5. Requirements for high-risk AI systems

- **Realistic and proportionate obligations** - The proposed obligations and requirements for high-risk AI applications seem overly prescriptive, burdensome, overreaching and difficult (if not impossible) to implement across the value-chain. Some of the requirements applying to high-risk systems have to better consider proportionality, feasibility and the need to be adapted to the specific situation. This approach is consistent with the risk-based approach whereby organisations can calibrate the requirements to the specific AI system and the risk involved. CIPL suggests that the final AI Act be more explicit about the risk-based approach by expressly providing that the requirements for high-risk AI are properly calibrated on the basis of the risk assessments performed by the organisation as part of the risk management system provided for in in Article 9. This will ensure the obligations set by the Act can be implemented in a practical, fair, and realistic manner.

- **Principle- and outcome-based requirements -** The impact of the AI Act requirements for high-risk AI should be taken into account to avoid hampering innovation, especially for SMEs. To address this, CIPL believes the requirements should be more results-oriented, i.e. focusing on "what" are the goals to be achieved, rather than on "how" to achieve compliant high-risk AI, with the underlying objective of minimising bureaucratic burdens for EU companies innovating in the AI field.[7] By focusing on "desired

[7] See the recent Open Loop project that gathered ten AI start-ups from diverse sectors to conduct AI impact assessments related to their AI products, based on principle-based regulation and procedural regulatory guidance. All of the participants were better able to identify the risks posed by their AI application based on practical regulatory guidance, mitigate these risks and embed best practices and safeguards in the design of their products. This resulted in greater efficiency and faster delivery to market, while reducing costs and risks of later disruption.

outcomes" rather than on "prescriptive requirements", the AI Act would help achieve the objective of fostering the development and uptake of AI while respecting EU values and fundamental rights.

- **Error-free and complete data sets:** As currently phrased, this requirement appears as an unrealistic standard because:

    - Supervised learning relies on large quantities of human-labeled data. Even if it were possible to define completely unambiguous categories, any human-driven process would contain mistakes. Moreover, in most instances, it is impossible to have completely unambiguous categories, meaning that even the most expert human labelers will disagree and make mistakes. An error-free standard would make supervised learning impossible;

    - Unsupervised learning does not use human-labeled data, but is a machine learning approach that iteratively looks for patterns in large, unstructured data sets. This process is, by definition, imperfect. However, an error-free standard might foreclose some of the most promising advancements in AI research;

    - The best AI systems are robust and accurate even when there are errors in the data sets. Because no data set can ever be error-free, AI systems are designed to operate robustly when they encounter imperfect data. For that reason, the focus on error-free data in the AI Act is misplaced; it is more important to focus on the overall impacts of the system as a whole;

    - No data set is ever complete. There is always more data that could be collected, but collecting additional data creates greater privacy risks for individuals; and

    - These requirements would be all the more difficult to comply with by the provider of an AI system that is only fed with client data, and not the provider's data.

  Consequently, these obligations should be removed or at least, the language pertaining to these obligations should be phrased as ensuring best efforts or abiding by industry standards.

- **Publicly accessible data base** - The Act provides for the creation of a publicly accessible database to register high-risk AI applications (including meaningful information about the AI systems and the conformity assessment carried out on those systems). There have been calls to expand this database to low-risk uses. CIPL believes that would not be the right approach as it would create a substantial reporting and administrative burden for AI providers, particularly as AI is integrated into more and more systems. Additionally, it would potentially require AI providers to disclose sensitive business information, to the detriment of business competitiveness. Transparency as a cornerstone to trustworthy AI must be balanced with the need to ensure that intellectual property and proprietary information remain protected, and that malicious actors are not encouraged to game the AI system.

Finally, extending the database to low-risk AI uses may not provide significant benefits to individuals whose fundamental rights are already protected by other regulations.

- **Revealing of source code -** As currently phrased, the AI Act requires the sharing of source code for market surveillance purposes in certain instances. CIPL agrees that providing relevant information is important to the proper monitoring and oversight of AI systems, particularly as a mechanism for giving regulators meaningful, usable, and actionable information. Such disclosure however, must be done without creating unnecessary risks to users or disclosing proprietary information or trade secrets, and must be in line with existing legislation (such as the trade secrets Directive). CIPL believes that more effective and meaningful guidance on how to enable access to this information should be developed together with industry.

- **Addressing Bias -** The AI Act focuses on bias in data sets, but bias can be a challenge throughout the lifecycle of an AI system, not simply in data sets. The Act should consider, from a holistic perspective, whether an AI system is biased, rather than focusing exclusively on data sets. In addition, it is important that the AI Act specifically allows companies to process sensitive data under the GDPR for purposes of measuring and mitigating bias in all AI systems (and not just high-risk AI systems).

- **Assessing inclusivity** - Stronger commitments to using AI to drive inclusivity should be included. Although Article 10(5) of the Act acknowledges that processing of special categories of personal data may be required "for the purposes of ensuring bias monitoring," CIPL questions whether this goes far enough in terms of guarding against bias or proactively promoting inclusivity, and whether assessments should also have a particular focus on assessing impacts on vulnerable groups.

6. **Transparency**

- **Meaningful transparency** - CIPL agrees that individuals need to be empowered through appropriate transparency, control, and choice. Such transparency, however, needs to be properly balanced in order to empower individuals without overwhelming them. For example, transparency for transparency's sake may lead to a report that is incomprehensible to the average individual who is not an AI expert. Therefore the AI Act needs to ensure that the nature of the audience is considered when the proper level of transparency is defined.

- **Lack of universal practical standards** – Due to the lack of standards to address AI considerations holistically, it is important that policymakers work collaboratively with experts from industry to ensure an appropriately balanced approach. Many AI systems at issue are profoundly complex, often the result of the combined effort of thousands of engineers around the world, and there are unanswered questions about how to provide meaningful transparency about these complex systems while preserving privacy and trade secrets. In addition, organisations may have to make trade-offs between considerations such as transparency of the AI system and its security or accuracy. There exists a range of emerging approaches to documenting machine learning systems, such as "model cards" and "data

set nutrition labels," that can potentially provide a snapshot of how a system was developed and how it performs. These tools, however, are still being developed. There are no clear standards for such documentation efforts, nor have they yet been demonstrated to be practical at a meaningful scale.

7. Conformity assessments

- **Self-assessments** – CIPL believes that relying on organisations' self-assessments for most high-risk AI systems strikes a good balance between innovation and the preservation of fundamental rights. Requiring prior approval for all high-risk AI systems would be harmful to innovation (especially as the Commission notes that expertise for AI auditing is only now being accumulated). Many organisations have already established self-assessment processes in the context of GDPR and will be able to leverage them for high-risk AI assessment purposes.

- **No double reporting** – CIPL underlines that it would be overly burdensome for all products that require conformity assessments under legislation listed in Annex II to also be subject to additional AI-specific requirements set out in the AI Act. Some video conferencing products' endpoints, for example, require conformity assessments under the Radio Equipment Directive listed in Annex II of the AI Act. The use of AI in such systems is intended to enhance collaboration between employees and is therefore unlikely to be high-risk. Although the infrastructure with conformity assessment bodies is well-established and efficient, it will be essential to make sure that there is no double reporting requirement and that these bodies are properly equipped to deal with this new role.

8. Regulatory Sandboxes

- **More clarity** – CIPL welcomes the inclusion of a legal basis for regulatory sandboxes in the AI Act. The relevant provisions should be underpinned by clear and unambiguous rules for those making use of sandboxes, including sufficient guidance to regulators about their operation, and the need for consistency in approaches. In particular, the provisions should address how insights and learnings obtained from the regulatory sandbox exercises can inform the policy making process of the AI Act (including modifications to the Annexes), as well as its enforcement.

- **Incentives -** The AI Act needs to more clearly lay out the incentives for organisations to join sandboxes and the outcomes they can expect.[8] CIPL encourages the Commission and the relevant regulators to work with industry to: (1) think about the specific functioning of sandboxes; (2) set them up in a way that truly helps companies to drive innovation in a protected environment to unearth learnings for all stakeholders involved; and (3) enable sandboxes to reach beyond SMEs and be made more inclusive.[9]

[8] See CIPL Paper Regulatory Sandboxes in Data Protection – Constructive Engagement and Innovative Regulation in Practice.

[9] The AI Act currently prioritises regulatory sandboxes to small-scale providers and start-ups. The possible impact on a level playing field needs to be assessed as sandboxes can only take in a number of applications at any given time, and this is likely to be far smaller a number than the amount of AI innovations being developed in the market place.

- **Testing legislative and regulatory approaches** - Regulatory sandboxes are important mechanisms for regulatory exploration and experimentation as they provide a test bed for applying laws to innovative products and services in the AI field. At the same time, given that there are so many unanswered questions surrounding AI governance, it is quite challenging to design and assess the most appropriate, feasible and balanced legislative instruments. Collaborative, multi-stakeholder policy prototyping can provide a safe space to explore, assess and develop different legislative models of governance prior to their actual enactment. Such tools may help to inform legislative and policy choices that are more suited to the quickly developing technology industry.[10]

9. <u>European Artificial Intelligence Board</u>

- **Industry representation** - CIPL welcomes the creation of the European Artificial Intelligence Board to enable ongoing collaboration between policy makers, industry, academics and researchers. This collaboration is essential as nascent AI technology develops further and new use cases, opportunities and challenges are unearthed. However, CIPL would like to see a more systematic participation of industry as part of the Board's permanent structure. Article 57 of the Act only provides that it may invite external experts and observers to attend its meetings, and may hold exchanges with interested third parties to inform its activities to an appropriate extent.

10. <u>Governance mechanism</u>

- **Single point of contact** - The proposed governance and enforcement mechanism is highly complex and may result in an inconsistent application of the AI Act in the EU. This may create uncertainty for systems trained and operating across borders and discourage investments in AI because of possible uncertain and inconsistent regulatory outcomes. CIPL recommends having a mechanism that would set up a single point of contact for organisations for each AI system.

- **Keep the competence of existing regulators -** In reference to the language that national states may appoint (and draw upon the expertise of) existing sectoral authorities and entrust them also with the powers to monitor and enforce the provisions of the regulation, CIPL supports existing sectoral authorities retaining supervision. For purposes of legal certainty, DPAs should retain general competence over AI applications involving the processing of personal data and/or impacting individuals' privacy and other human rights. As such, they should be in a leading position and the single point of contact for the organisation in question, but with the ability to collaborate with other authorities where necessary. For instance, where AI does not involve the processing of personal data (e.g., AI used for manufacturing processes), the authority with the most relevant expertise (e.g., because of the sector in which the AI is deployed) could take the lead and cooperate with other authorities where needed.

[10] See note 7.

- **Promote responsible AI practices -** The AI Act should also consider how to promote, incentivise and reward industry best practices and responsible approaches to AI development and use. Such "incentives" could include for instance recognising self-regulatory commitments of organisations that publicly define the AI values and principles they implement along with progress against benchmarks, using demonstrated accountability as a "licence to operate" by allowing accountable and/or certified organisations greater opportunities to use and share data responsibly or using demonstrated AI accountability as a criterion for public procurement projects.[11]

11. Reporting obligations

- **Reporting of serious incident and malfunctioning** – Article 62 would require the reporting to market surveillance authorities of any serious incident or any malfunctioning that constitutes a breach of obligations under EU law. As it stands, the provision is excessively broad. While the concept of "serious incident" is sufficiently limited in scope, that of "malfunctioning" is not. This term lacks qualifiers and could be given broad meaning to apply to any circumstance in which the AI system does not perform as intended. This threshold seems unreasonably low and would create large administrative costs for AI providers that would have to closely monitor and report all cases of malfunctioning. This low threshold would also create huge workloads for market surveillance authorities that would have to assess and decide on appropriate measures in such cases. Therefore CIL recommends limiting the reporting obligation to serious incidents and to instances of serious malfunctioning that breach EU law.

- **Risk of double reporting obligations** – CIPL also flags the potential risk of overlapping reporting obligations under different EU laws. It is possible that a serious incident involving an AI system could give rise to reporting obligations under the AI Act and under the NIS Directive or the GDPR, for instance. However, each of these instruments specify different reporting times and require that notification be made to different regulators, who will be tasked with assessing the incident and deciding on appropriate measures, including investigations. CIPL recommends that Article 62 be revisited to account for the duplication of reporting duties, and, where overlapping obligations exist, clarify which reporting system applies under which circumstances.

12. Interaction of the AI Act with the GDPR

- **Relation between the AI Act and the GDPR** - The AI Act is largely an instrument of product law, but makes multiple references to, and impacts, fundamental rights, including data protection. While it appears that there is no intent to construct the AI Act as *lex specialis* to the GDPR, CIPL underlines the necessity to ensure that the AI Act does not have the unintended effect of creating additional or conflicting rules with respect to personal data, including cases where AI applications do not interfere with data protection while bringing benefits to society.

[11] See note 3 at page 8 for more examples of possible incentives.

- **Duplication of obligations** – CIPL highlights that it would be a concern for businesses if the AI Act imposes duplicative compliance efforts or additional "red tape." For example, for models that use personal data, it should be expected that organisations can leverage their obligations to perform a data protection impact assessment (DPIA) under Article 35 of the GDPR as part of the obligation to have a risk management system in place under Article 9 of the AI Act.

- **Processing of special categories of personal data** – Article 10(5) of the AI Act appears to introduce an additional exemption for processing special categories of personal data in the context of monitoring bias in AI systems. CIPL would welcome clarification on this provision, particularly with respect to whether Article 9(2) the GDPR will be amended to include processing of personal data for bias monitoring, detection and correction in high-risk AI systems. If this is not the case, CIPL would welcome clarification as how to reconcile the two regulations.

- **Alignment of legal regimes** - The AI Act should be fully aligned with GDPR for AI systems that process personal data. In particular, the following provisions should be aligned:(1) Article 5 on the principles related to the processing of personal data; and (2) Article 22 on automated individual decision-making, including profiling. Certain AI applications currently allowed under Article 22 of the GDPR may be prohibited or deemed high-risk under the proposed AI Regulation, raising legal questions.

13. <u>Extra-territoriality</u>

- **Overly broad outreach** - The AI Act risks creating legal uncertainty with respect to providers and users of an AI system located outside the EU. Recital 11 provides that certain AI systems should fall within the scope of the AI Act even when they are neither placed on the market, nor put into service, nor used in the EU. This appears to be an overly broad approach.

- **Use of the output of an AI system in the EU -** Article 2(3) captures a scenario where the AI provider and users are outside the EU and the output is used in the EU without defining "output." CIPL would welcome additional clarity on the definition of output, and, in particular, whether it is intended to mean insight, algorithm or a set of data points. This clarification would be particularly critical in the field of medical research, where studies performed in one country can result in conclusions that are applied globally. CIPL underlines that in practice it is difficult to know when a study may have far-reaching impacts, and when it might be necessary to plan for compliance with EU regulations when research is undertaken outside of the EU.

14. International cooperation

- **Global AI governance** - The AI Act needs to be drafted with consideration that it will be used as global blueprint for lawmakers and regulators already examining AI, as well as a start for a global discussion around AI governance.[12] CIPL would like to see more explanation of how the EU intends to collaborate on AI governance on an international level. Globally consistent rules or principles include a number of benefits, including greater clarity to individuals in understanding what their rights are in respect of AI technologies. Having fragmented rules across different regions risks adding complexity and creates the possibility for confusion – particularly for organisations building models, including SMEs. Having a single set of global principles, such as those being reviewed by OECD,[13] may help to support consistency, drive confidence, lower costs and enable competition. Without a carefully coordinated approach, organisations operating internationally may face a complex and potentially conflicting set of rules.

- **Promotion of global voluntary industry-driven standards -** The history of AI development and AI standards has been one of collaboration – between many different actors from businesses, universities, research organizations and others – and between countries around the world. It is important that the EU continues to further promote that collaborative approach to unlock the full potential of AI. These standards, created by technical experts, enable commonality and reduce fragmentation on technical aspects, quality management, governance and risk management of AI. They are designed to be flexible and to foster innovation without being too prescriptive, while helping achieve outcomes on transparency, privacy, cybersecurity, safety and resilience in a global market.

CIPL is grateful for the opportunity to provide input on the Draft AI Act. If you would like to discuss these recommendations or require additional information, contact Bojana Bellamy, bbellamy@huntonAK.com, Markus Heyder, mheyder@huntonAK.com, or Nathalie Laneret, nlaneret@huntonAK.com.

[12] See for instance in the U.S., where the Federal Trade Commission has spotlighted its interest in AI
[13] See https://www.oecd.org/going-digital/ai/principles/