CIPL
Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Summary of Recommendations for Defining a Regulatory Path for AI in the EU: How to Leverage the GDPR, Accountability and Regulatory Innovation in AI Development, Deployment, and Uptake

Building on its prior work on organisational accountability and accountable AI in data protection, the Centre for Information Policy Leadership (CIPL)[1] started to work in February 2020 on a new project to develop recommendations in response to the EU Commission's White Paper on AI[2] as well as to continue to provide input into the ongoing policy and law development process following the initial white paper. Working with AI experts and a group of EU and multinational companies that are leaders in AI, CIPL's aim is to inform the discussions on development on AI rules, best practices and regulation in the EU and provide pragmatic evidence on emerging trends in building and delivering accountable and trustworthy AI. CIPL produced two position papers so far: "How the General Data Protection Regulation (GDPR) Regulates AI"[3] and CIPL's Response to the EU Commission White Paper - How to Leverage the GDPR, Accountability and Regulatory Innovation in AI Development, Deployment, and Uptake.[4] This short Paper is a summary of the recommendations we make in these two CIPL papers.

CIPL recommends a layered approach to regulating AI comprising: **(1)** a minimal, principles-based, outcome-based and risk-based approach, relying on existing laws and standards; **(2)** risk-based, demonstrable and verifiable accountability measures and practices of organisations; and **(3)** smart regulation and oversight, based on co-regulatory instruments, regulatory sandboxes and regulators' hubs.

As a preliminary remark, CIPL recommends that the following overarching principles be considered:

- **Build on the existing legal frameworks and adopt a minimalist approach to regulating AI:** many risks are not AI-specific (AI may simply amplify the risk) and are already addressed by existing laws which provide for baseline structures, requirements, tools and remedies;

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 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 at http://www.informationpolicycentre.com/. 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] CIPL's Response to the EU Commission White Paper - How to Leverage the GDPR, Accountability and Regulatory Innovation in AI Development, Deployment, and Uptake (June 2020). https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_eu_consultation_on_ai_white_paper__11_june_2020_.pdf CIPL's response provides recommendations for the future AI regulatory framework with a focus on risks for fundamental rights, personal data, privacy protection, non-discrimination and safety. It does not specifically cover the liability and compensation regime.

[3] Available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf

[4] See note 2.

- Ensure timely **involvement of all EU stakeholders in discussions around AI regulation**, including ethicists, lawyers, data scientists, engineers, privacy and security experts, computer scientists, epistemologists, statisticians, AI researchers, business leaders and public sector representatives;

- Benchmark **approaches outside the EU, for example the OECD Principles on AI,** to promote globally harmonised and interoperable guidelines on AI where possible;

- Align with the Commission's approach to **defining a framework for data access and use;**[5]

- Promote the **development and implementation of best practices** by all stakeholders in the AI ecosystem, with the objective of **continuous improvement** and **risk mitigation**.

1. A minimal, principles-based, outcome-based and risk-based approach, relying on existing laws and standards

1.1. To maximise AI benefits for the EU economy and societies while minimising its risks and to ensure a futureproof framework for the fast developing AI technology and systems, the regulatory approach must be risk-based. This means:

a. **First,** the general AI legal framework should encompass only high-risk AI applications. Such high-risk AI is identified by AI impact assessments performed by organisations that take into account the context and impact of a proposed use of AI (rather than its inherent type or the sector it is utilised in – as sectors are not static and clearly delineated). Further, any examples or illustrations of high-risk AI should be treated as rebuttable presumptions of what might constitute high-risk AI rather than rigid pre-defined classifications. This would give organizations the opportunity to demonstrate that specific AI applications are not, in fact, high-risk under the circumstances at hand. Importantly, organisations must also assess the overall impact of the AI application, including its benefits and the potential risk of not using it, rather than focusing on direct risk only.

b. The GDPR may assist in identifying the **possible indications of high risk AI**. Recital 75 provides guidance on what is considered risky or high-risk processing.[6] Article 22 defines the

[5] The European strategy for data calls for "*an agile approach to governance that favours experimentation*" over "*heavy-handed ex ante regulation*" https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

[6] *The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

requirements applicable to solely automated decision making and in doing so, it relies on the legal effects of the decision concerning an individual or on the effects that similarly significantly affect an individual. On this basis, CIPL has classified different types of data processing and AI uses that would or would not result in producing legal effects or similarly significant effects on individuals (See Appendix 2).[7]

c. **Second,** the actual principle-based requirements applicable to a particular AI application should be calibrated on the basis of their risks to individuals. Higher risk AI should require stronger protections and be subject to additional rules to mitigate the risks. Importantly, not all protections may be relevant in all circumstances and some trade-offs on the different protections may have to be made on a case-by-case basis.

1.2 **Prior consultation** with regulators should be limited to the most risky AI uses where risk cannot be mitigated, to avoid burdensome, inefficient and lengthy administrative procedures, not suited for fast-paced development of AI technologies and systems.

1.3 AI rules should **not duplicate or conflict with the GDPR requirements**, but build on its existing rules and the practices developed by organisations (such as Data Protection Impact Assessments to identify and address processing of data that is likely to result in a high risk to the rights and freedoms of natural persons). This will not only avoid legal uncertainty that could have a chilling effect on development and deployment of AI in the EU, but also enable organisations to leverage their current efforts in complying with the GDPR's risk-based approach for AI.

2. Risk based, demonstrable and verifiable accountability measures and practices of organisations

2.1 Rather than imposing prescriptive requirements, the law should **provide principle- and outcome-based rules** which help organisations achieve specified goals (e.g. fairness, transparency, accuracy, human oversight) through concrete, demonstrable and verifiable risk-based measures.

2.2 There should be a specific accountability requirement as follows: *"Taking into account the nature, scope, context, purposes, impact, risks and benefits of an AI application, **the organisation shall implement, and be able to demonstrate** that it has implemented, appropriate organizational and technical policies and measures to comply with the principles in the AI Regulation. Organisations will review and update such policies and measures where necessary."* This enables organisations to define and tailor the type and strength of the measures that are needed to reach the required outcomes on the basis of their own assessment, industry best practices, regulatory guidance, or external technical standards (such as for instance the HLEG Trustworthy AI self-assessment list). These accountability measures are de facto mandatory within the organisation and are reviewed and potentially updated on a regular basis to take into account the dynamic character of AI. Accountability can also be certifiable by third party certifiers. This approach can provide more effective protections for individuals and society in the context of AI, while driving the benefits of AI technologies and building EU AI capabilities, especially with SMEs.

[7] CIPL's comments on the Article 29 Data Protection Working Party's "Guidelines on Automated Individual Decision-Making and Profiling" (December 2017) on page 6.

2.3 The regulatory regime should provide appropriate rewards and encouragements to stimulate and help accelerate demonstrable and certifiable AI accountability and best practices of organisations, such as for instance: promoting organisational accountability through Digital Innovation Hubs; using demonstrated accountability as a "licence to operate" by giving accountable organisations greater freedom to use and share data responsibly to facilitate growth in responsible AI; allowing broader use of data in AI for social good projects; using demonstrated and/or certified AI accountability as a criterion for public procurement projects; using demonstrated and/or certified AI accountability as a mitigating factor or as a liability reduction factor in the enforcement context.

3. Co-regulatory instruments and innovative regulatory oversight

3.1 Rather than create a new AI regulator, the oversight of AI practices should be based on the **current ecosystem of sectoral and national regulators.** This means: **a)** keeping the competence of national data protection authorities intact when AI involves the processing of personal data, and **b)** setting up an EU governance structure of regulatory hubs composed of AI experts from different regulators to avoid fragmentation and drive consistent application of the rules, including where AI has a cross-border and/or cross-sectoral impact. AI expertise and acumen of existing authorities must be expanded, rather than creating new structures.

3.2 This approach should be complemented by a **consistent EU-level scheme of voluntary codes of conduct, certifications and labeling.** These must be designed through consultation with stakeholders and updated regularly based on technological developments and new practices. They help increase trust that an AI application meets certain criteria that have been assessed by an independent body. They should also be designed with a view of ensuring maximum interoperability with non-EU certification schemes and labels, to make it easier for EU multinational companies to compete globally on AI technologies and systems.

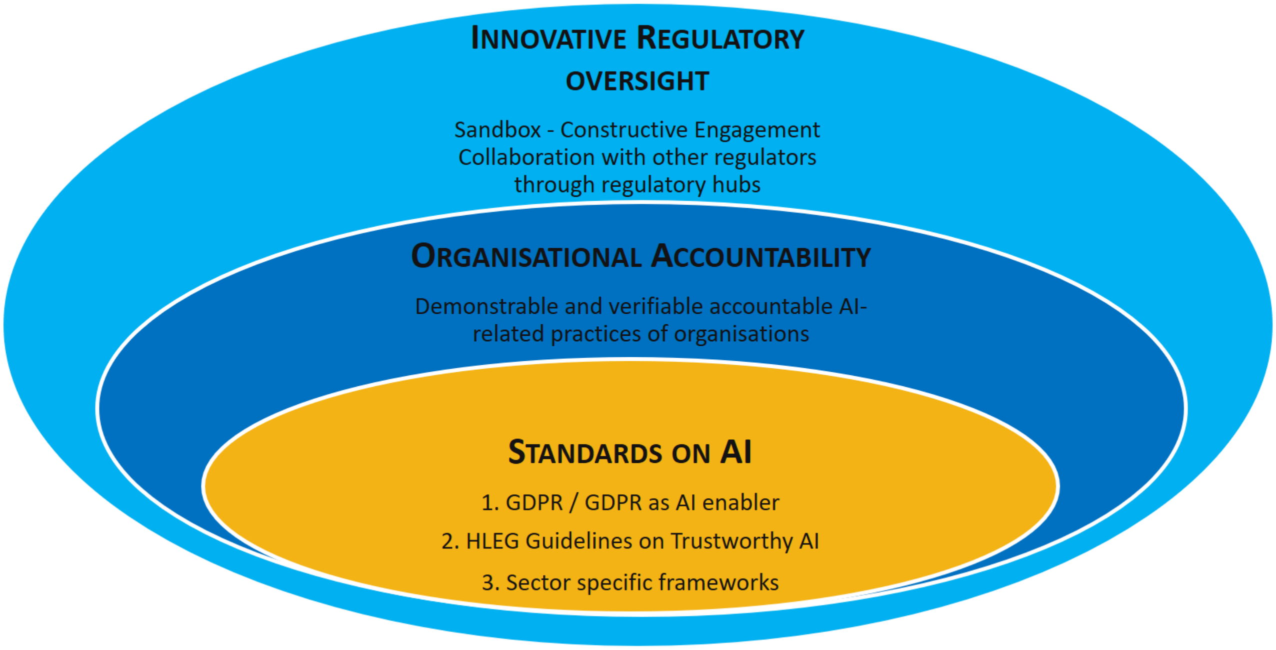
3.3 The EU AI regulatory framework must provide an explicit statutory basis for innovative regulatory oversight tools, such as data review boards and regulatory sandboxes. This would apply to relevant data protection authorities and other sectoral regulators overseeing the application of AI regulation.

a. **Data review boards** are standing committees (whose characteristics may be defined by regulators) that are convened according to certain risk indicators to promote a thoughtful dialogue and consideration of risks and benefits in relation to high-risk AI projects.

b. **Regulatory sandboxes** provide supervised "safe spaces" to organisations for building and piloting innovative AI uses in a reiterative manner and with open and constructive collaboration with, and feedback from, regulators to ensure accountable and trustworthy innovation.[8]

[8] See CIPL Paper "Regulatory Sandboxes in Data Protection – Constructive Engagement and Innovative Regulation in Practice - March 8, 2019 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_-_constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf

Appendix 1 - CIPL’s Layered Approach to Regulating AI in the EU



INNOVATIVE REGULATORY OVERSIGHT

Sandbox - Constructive Engagement
Collaboration with other regulators
through regulatory hubs

ORGANISATIONAL ACCOUNTABILITY

Demonstrable and verifiable accountable AI-related practices of organisations

STANDARDS ON AI

1. GDPR / GDPR as AI enabler
2. HLEG Guidelines on Trustworthy AI
3. Sector specific frameworks

Appendix 2 - CIPL Table on the Application Threshold of Article 22 GDPR

Decisions Producing Legal Effects	• Decisions affecting the legal status of individuals • Decisions affecting accrued legal entitlements of a person • Decisions affecting legal rights of individuals • Decisions affecting public rights — e.g. liberty, citizenship, social security • Decisions affecting an individual's contractual rights • Decisions affecting a person's private rights of ownership
Decisions Producing Similarly Significant Effects *Some of these examples may also fall within the category of legal effects depending on the applicable legal regime and the specific decision in question*	• Decisions affecting an individual's eligibility and access to essential services — e.g. health, education, banking, insurance • Decisions affecting a person's admission to a country, their citizenship, residence or immigration status • Decisions affecting school and university admissions • Decisions based on educational or other test scoring – e.g. university admissions, employment aptitudes • Decision to categorise an individual in a certain tax bracket or apply tax deductions • Decision to promote or pay a bonus to an individual • Decisions affecting an individual's access to energy services and determination of tariffs
Decisions Not Producing Legal or Similarly Significant Effects *These automated decisions do not typically produce such effects. Instances where they might produce such effects are contextual and should be determined on a case-by-case basis.*	• Decisions ensuring network, information and asset security and preventing cyber-attacks • Decisions to sandbox compromised devices for observation, restrict their access to or block them from a network • Decisions to block access to malicious web addresses and domains and delivery of malicious emails and file attachments • Decisions for fraud detection and prevention (e.g. anti-fraud tools that reject fraudulent transactions on the basis of a high fraud score) • Decisions of automated payment processing services to disconnect a service when customers fail to make timely payments • Decisions based on predictive HR analytics to identify potential job leavers and target them with incentives to stay • Decisions based on predictive analytics to anticipate the likelihood and nature of customer complaints and target appropriate proactive customer service • Normal and commonly accepted forms of targeted advertising • Web and device audience measurement to ensure compliance with advertising agency standards (e.g. requirements not to advertise foods high in fat, sugar and sodium when the audience consists of more than 25 % of children)