Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

CIPL Webinar:

Latest Trends in AI Regulation and Organizational Approaches to Accountable AI

26 March 2020

A Global Privacy and Security Think Tank

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

BRIDGING REGIONS | BRIDGING INDUSTRY & REGULATORS | BRIDGING PRIVACY AND DATA DRIVEN INNOVATION

ACTIVE GLOBAL REACH

90+ Member Companies

5+ Active Projects & Initiatives

20+ Events annually

15+ Principals and Advisors

We **INFORM** through publications and events

We **NETWORK** with global industry and government leaders

We **SHAPE** privacy policy, law and practice

We **CREATE** and implement best practices

ABOUT US

- The Centre for Information Policy Leadership (CIPL) is a global privacy and security think tank
- Based in Washington, DC, Brussels and London
- Founded in 2001 by leading companies and Hunton Andrews Kurth LLP
- CIPL works with industry leaders, regulatory authorities and policy makers to develop global solutions and best practices for data privacy and responsible use of data to enable the modern information age

Twitter.com/the_cipl

https://www.linkedin.com/company/centre-for-information-policy-leadership

www.informationpolicycentre.com

2200 Pennsylvania Ave NW
Washington, DC 20037

Park Atrium, Rue des Colonies 11
1000 Brussels, Belgium

30 St Mary Axe
London EC3A 8EP

Welcome and Introductions

Bojana Bellamy

President, CIPL

Ali Shah

Head of Technology, UK Information Commissioner's Office

Caroline Louveaux

Chief Privacy Officer, Mastercard

William Malcolm

Privacy Legal Director, Google

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Regulatory State of Play for AI

EU Commission Considering AI Legislation

- Open consultation: White Paper on AI – A European Approach to Excellence and Trust (deadline: 31 May 2020)
- CIPL planning to respond

Key Regulatory AI Initiatives

- UK ICO AI Auditing Framework
- Commission HLEG on AI Assessment List Pilot
- Canada OPC Consultation: Proposals for Ensuring Appropriate Regulation of AI (recently concluded 13 March 2020)

Regulatory Sandbox

- UK ICO Beta Phase
- Endorsed in AI strategies
  - South Korea
  - Finland
- Endorsed in legislation
  - Malta
  - India

Plethora of Regulatory Guidance

European Union

- UK ICO
- CNIL
- Norway Datatilsynet
- Commission HLEG on AI
- Council of Europe

Elsewhere

- Singapore PDPC
- OECD
- US Office of Management and Budget

CIPL Work on AI

Delivering Sustainable AI Accountability in Practice

To learn more about the project, see https://www.informationpolicycentre.com/ai-project.html

First Report
Artificial Intelligence and Data Protection in Tension

10 October 2018
https://bit.ly/2RjxonR

- **Details the widespread use, capabilities and potential of AI applications**
- **Examines tensions between AI technologies and some data privacy legal requirements**

Second Report
Hard Issues and Practical Solutions

28 February 2020
https://bit.ly/399Pn63

- **Dives deeper into some of the hardest challenges of AI and data protection and puts forward concrete approaches to mitigating the tensions**
- **Outlines best practices and tools that organizations are currently developing to enable accountable and human-centric AI**

New Initiative
EU AI Project

2020 Onwards

- **CIPL layered approach to regulating AI**
- **Responding to EU Commission AI white paper on "A European approach to excellence and trust"**
- **CIPL/Hunton Andrews Kurth paper on GDPR and AI**
https://bit.ly/39h1rlt

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

UK ICO's AI Auditing Framework

Developing an Artificial Intelligence Framework

Background, objectives and timeline

Framework objectives

- Develop a solid methodology for the ICO to assess the data protection compliance of AI systems.
- Support the development of internal knowledge, capabilities, and toolkits to support the work of the ICO, and in particular the assurance and investigations teams.
- Inform additional external guidance for organisations on how to manage data protection risks in AI systems

Why is it a priority for the ICO?

Many AI applications involve personal data and automated decisions

The complexity, speed and scale of the processing of personal data in AI systems may make risks more difficult to identify and/or manage, while increasing the potential detriment to data subjects.

- Accountability & Governance
  - DPIAs,
  - Controller / processor status,
  - Trade-offs
- Lawfulness, Fairness and Transparency
  - Lawful basis, statistical accuracy,
  - Bias and discrimination
- Security and Data Minimisation
- Enabling individual rights in AI

Some examples of tensions between data protection and AI

Data minimisation and accuracy	**Large data and complex sets required to train, test and deployment of AI systems**
Purpose limitation	**Often based on data collected for another purpose (e.g. crash analytics -> ad targeting)**
Transparency and fairness	**Low interpretability and explainability of complex AI models and applications**
Art. 22 restricts fully automated decision making with legal / significant effect	**Human input slows down and may result in less accurate / consistent decisions**

Just like organisations need to assess whether they have the right risk management and governance capabilities to deal with AI, so does the ICO

ico.
Information Commissioner's Office

Some of the topics we have looked at

- Automated decision making and the role of meaningful human reviews;
- Accuracy of AI systems outputs
- Security risks exacerbated by AI
- Explaining AI decisions
- Human bias and discrimination in AI systems
- Trade-offs
- The right to human intervention
- Data minimisation and privacy-preserving techniques in AI systems
- Privacy attacks on AI models
- Individual rights in AI systems
- DPIAs and AI

Who is the guidance for?

- The draft guidance is taking a risk-based approach, which means:
  - assessing the risks to the rights and freedoms of individuals that may arise when you use AI
  - and implementing appropriate and proportionate technical and organisational measures to mitigate these risks.
- Therefore we have targeted the draft guidance at roles who we think should be more aware of the risks.

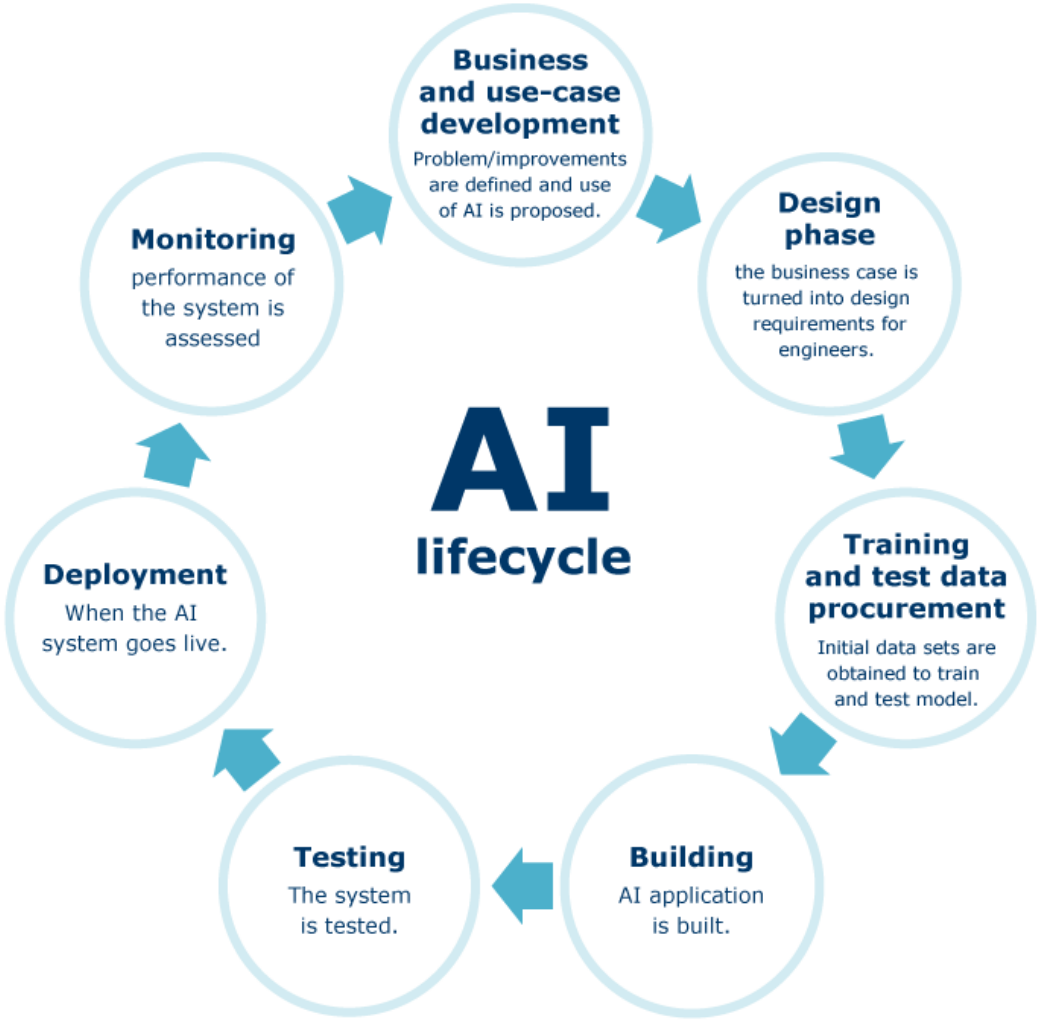
How is the guidance structured?

- Part one: governance and accountability
- Part two: Lawfulness, fairness and transparency
- Part three: security and data minimisation
- Part four: individual rights

How is the guidance structured?

- Preventative controls
  - Designed to stop errors or risks from happening
- Detective controls
  - Designed to find errors after they have occurred.
- Corrective controls
  - Designed to correct any errors found by the detective controls and mitigate the impact of the error.

Understanding what to do during the AI lifecycle



Some insights and open questions

- When is personal data personal data?
- Controller vs Processor
- Bias and discrimination
- Rights across the AI development lifecycle

- How to support those who are vulnerable, may have a disability, may require use of SCD to support?

What Next?

- Guidance consultation window is open
- We are ***extending*** the deadline for responses to ***1st May 2020***
- Final guidance to be released in **Summer 2020**

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Update on the State of Play of AI Regulation in Europe

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Responsible AI Deployment and Organizational Best Practices

Accountable AI | **Mastercard's Data Responsibility Imperative**

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Security & Privacy

Integrity

An organization's data practices

01 You Own It

You Control it 02

03 You Benefit from the Use of It

We Protect It 04

must be guided by the rights of individuals

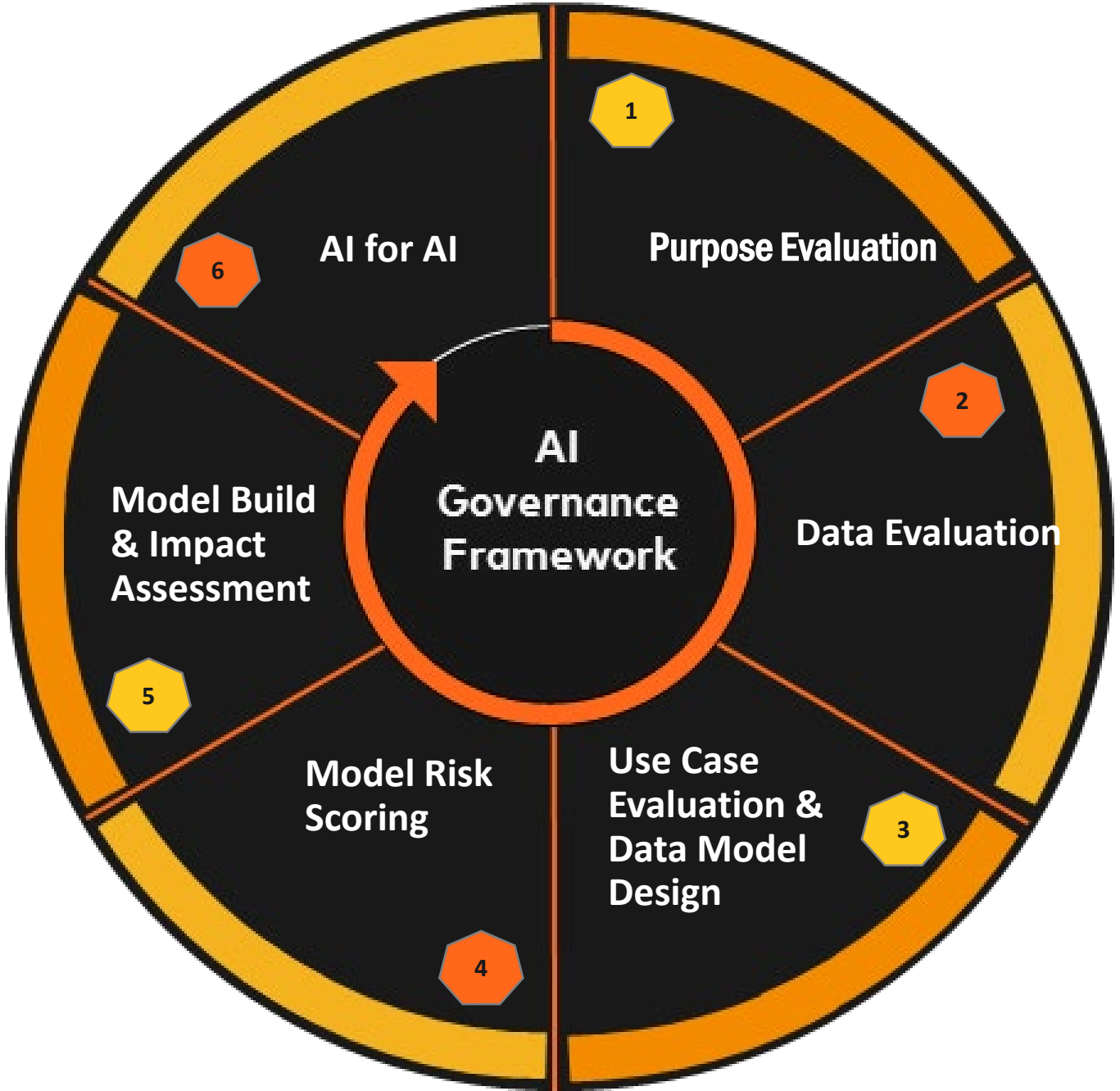
Accountability

Innovation

Transparency & Control

Social Impact

Accountable AI | Mastercard's AI Governance Framework



CIPL Accountability Framework

Organizations must be able to demonstrate accountability – internally and externally

Accountability is not static, but dynamic, reiterative and a constant journey

Accountability requires comprehensive privacy programs that translate legal requirements into risk-based, verifiable and enforceable corporate practices and controls

Company values and business ethics shape accountability

Examples of Best Practices in AI Governance

Mapped to Accountability

Leadership and Oversight

- Tone from the top to respect ethics, values and specific AI principles
- AI/ethics/oversight boards/committees
- Appointing responsible AI lead/officer
- Privacy/AI engineers and champions

Risk Assessment

- Algorithmic Impact Assessment
- Fairness assessment tools
- Risks and benefits assessment
- Document tradeoffs
- Anonymization techniques

Policies and Procedures

- Accountability measures for two stages – training and decision-making
- Pilot test AI models before release
- Assessment questions/procedures
- Due diligence checklists for business partners using AI tech and tools
- White, black, and gray lists of AI use
- Verification of data input and output

Transparency

- Differentiated transparency for different audiences/contexts
- Provide counterfactual information
- Factsheets and model cards
- Tiered transparency - Understand customers' expectations and deploy based on their readiness to embrace AI
- Transparency to individuals, DPAs, business partners and internally

Training and Awareness

- Data scientist training, including how to avoid and address bias
- Cross-functional training – privacy professionals and engineers
- Ad hoc and functional training
- Fairness training
- Ethics training

Monitoring and Verification

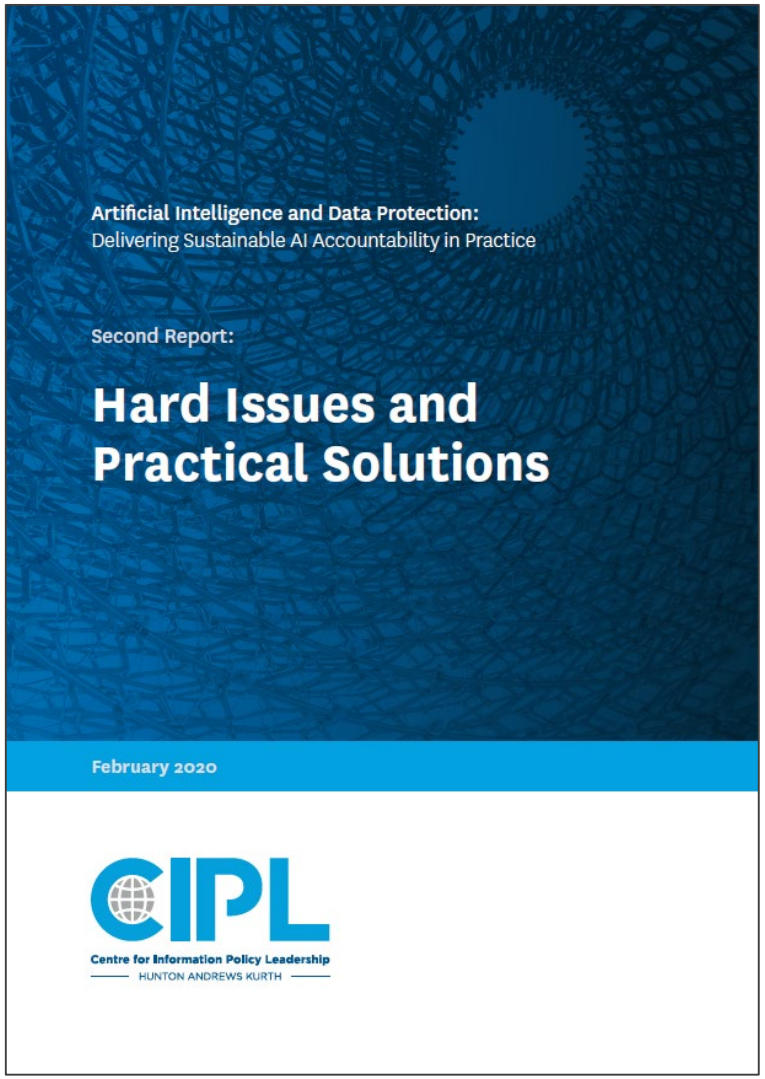
- Human in the loop—in design, in oversight, in redress
- Human understanding of the business and processes using AI
- Human audit of input and output
- Human review of individual decisions
- Ongoing monitoring, validation and checks

Response and Enforcement

- Complaints-handling
- Redress mechanisms for individuals to remedy AI decision
- Feedback channel
- Internal supervision of AI deployment

Hard Issues and Practical Solutions

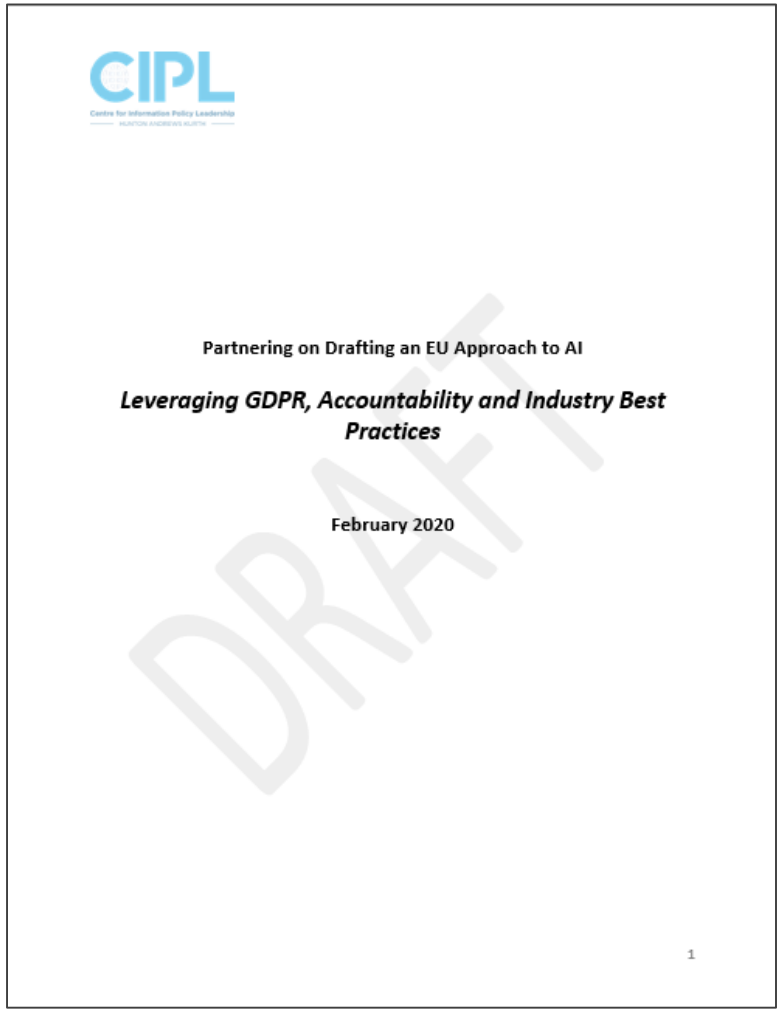
CIPL Second Report on AI – February 2020



- Follows CIPL's first report on "**Artificial Intelligence and Data Protection in Tension**"
- Dives deeper into some of the hardest challenges of AI and data protection (e.g. **fairness, transparency, purpose specification and use limitation, data minimization**)
- Puts forward concrete **approaches to mitigating some of the tensions** explored in first report
- **Outlines emerging best practices and tools** that organizations are currently developing to enable accountable and human-centric AI
- Maps best practices in AI governance to the **CIPL Accountability Wheel**

Response to EU Commission AI Policy Paper

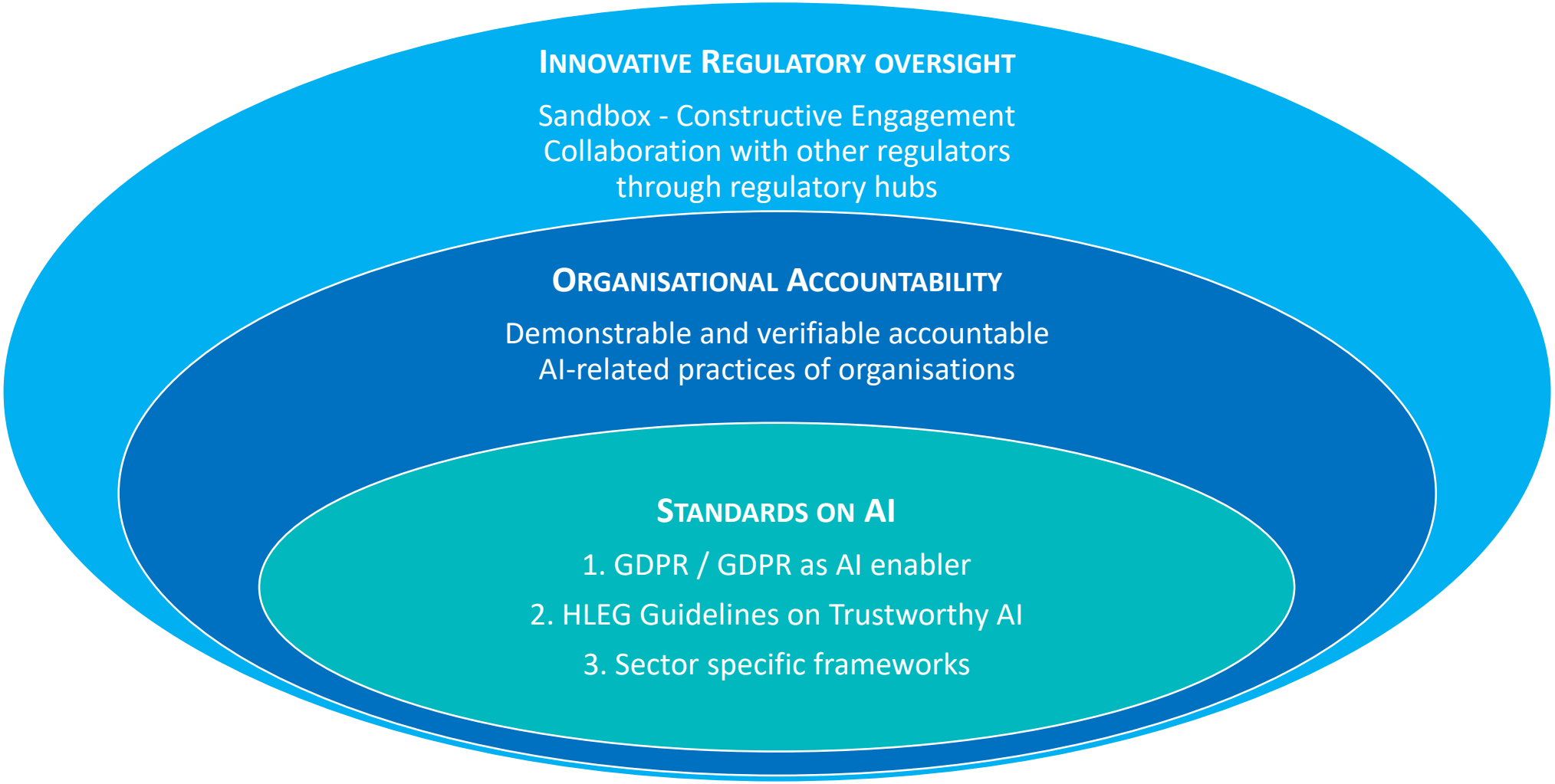
Leveraging GDPR, Accountability and Industry Best Practices



In this Paper, CIPL proposes a layered regulatory approach to AI that would leverage:

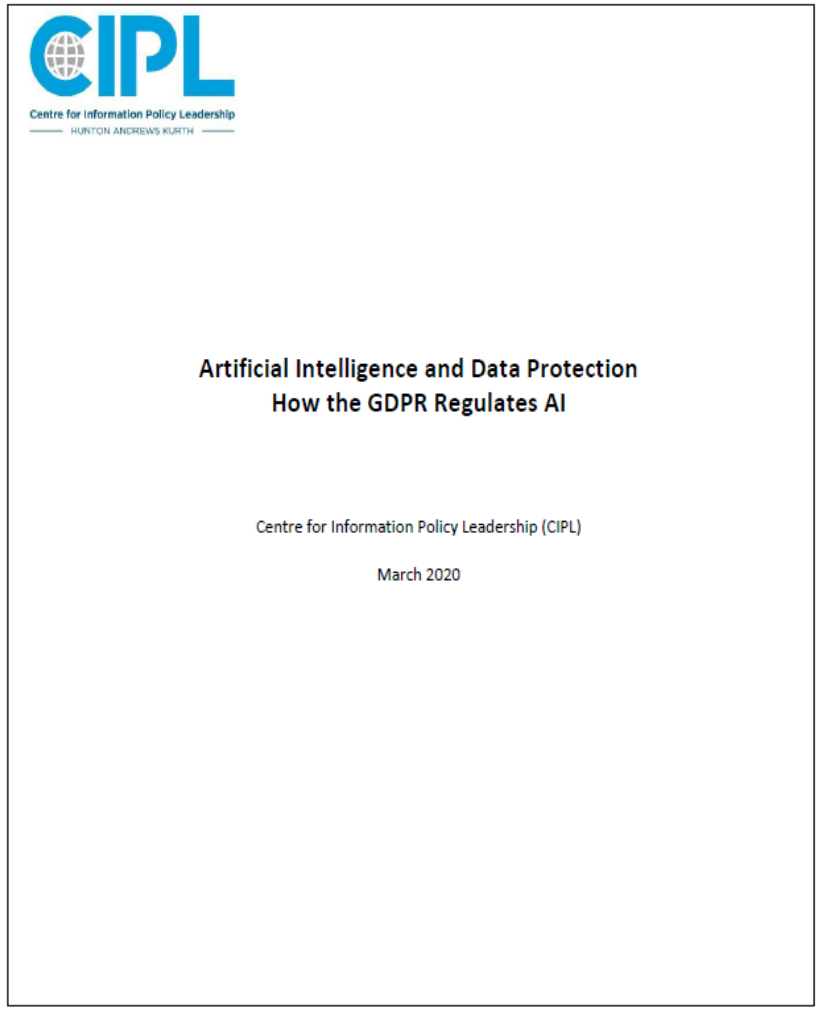
1. The GDPR framework and tools - help resolve the tensions between AI and GDPR
2. Demonstrable and verifiable accountable AI-related practices of organizations
3. Innovative approaches to regulatory oversight

CIPL Layered Approach to Regulating AI



How the GDPR Regulates AI

CIPL/HuntonAK Paper



The paper examines:

- **The applicability of the GDPR generally to AI** (e.g. through data protection principles, obligations on organizations and oversight of DPAs)
- **GDPR provisions that are of particular relevance in the context of AI** (e.g. requirement to carry out a DPIA where new technologies are used)
- **GDPR provisions that specifically regulate the use of AI** (e.g. right not to be subject to automated decision-making)

How GDPR Applies Generally in AI Contexts

CIPL/HuntonAK Paper

GDPR aims to be technology neutral and applies fully to the use of personal data in AI:

Article 3(2) Extraterritorial Effect	**Article 6(1)** Legal Basis	**Article 24(1)** Accountability	**Article 28** C to P Contracts	**Article 30** Records of Processing	**Articles 33 & 34** Data Breaches
Articles 15-21 Individual Rights	**Article 25** Privacy-by-Design and by-Default	**Article 46** International Data Transfers	**Article 37** DPO	**Chapters VII/VIII** DPAs, Enforcement and Sanctions	

GDPR Provisions of Particular Relevance to AI

CIPL/HuntonAK Paper

Several GDPR provisions are specifically relevant for AI:

Article 5(1)(a)
Fair Processing

Article 5(1)(c)
Data Minimization

Article 35
Conduct a DPIA for high-risk processing, in particular when using new technology

GDPR Provisions that Specifically Regulate AI

CIPL/HuntonAK Paper

Several GDPR provisions specifically regulate AI:

Article 13(2)(f)
Inform individuals of the existence of ADM and provide meaningful information about the logic involved (data collected directly)

Article 14(2)(g)
Inform individuals of the existence of ADM and provide meaningful information about the logic involved (data collected indirectly)

Article 15(1)(h)
Right to access information about the existence of ADM and meaningful information about the logic involved

Article 22
Right not to be subject to a decision based on solely ADM producing legal/similarly significant effects

Article 22(3)
Right to obtain human intervention and contest decision

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

EU Commission HLEG Guidelines for Trustworthy AI – Overlap with GDPR

Key requirements of Trustworthy AI	Overlap with GDPR provisions
Human Agency and Oversight	Legitimate interest balancing test (art. 6(1)(f)) / Transparency (art. 13 & 14) / ADM (art. 22) and Right to obtain human intervention (art. 22(3)) / Risk assessment and DPIA (art. 35)
Technical Robustness and Safety	Security (art. 32) / Risk assessment and DPIA (art. 35) / Data accuracy (art. 5(1)(d))
Privacy and Data Governance	Data protection principles (art. 5) / Legal grounds for processing (art. 6) / Legal grounds for sensitive data (art. 9) / Rights of the data subject (Chapter III) and in particular Transparency (art. 13 & 14) and Right to information on ADM and logic involved (art. 15(1)(h)) and Right not to be subject to an ADM decision (art. 22) and right to human intervention (art. 22(3)) / Accountability (art. 24(3)) / Data protection by design (art. 25) / Processor due diligence (art. 28(1)) / Security (art. 32) / DPO (art. 37 & 38)
Transparency	Transparency (art. 13 & 14) / ADM (art. 22)
Diversity, Non-Discrimination and Fairness	Fairness data protection principle (art. 5(1)(a)) / Risk assessment and DPIA (art. 35) / Right to information on ADM and logic involved (art. 15(1)(h))
Societal and environmental wellbeing	Risk assessment and DPIA (art. 35) / Transparency (art. 13 & 14)
Accountability	Accountability (art 5(2) & 24(3)) / Risk assessment and DPIA (art. 35) / Processor due diligence (art. 28(1)) / DPO (art. 37 & 38)

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Open Discussion

All participants are encouraged to submit questions and comments through the Q&A box in the Zoom Application

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Thank You

Bojana Bellamy
President, Centre for Information Policy Leadership
bbellamy@HuntonAK.com

Centre for Information Policy Leadership
www.informationpolicycentre.com

Hunton Andrews Kurth Privacy and Information Security Law Blog
www.huntonprivacyblog.com

@THE_CIPL

linkedin.com/company/centre-for-information-policy-leadership