Centre for Information Policy Leadership
HUNTON

CIPL response to the UK Government's Consultation: Data regulation in the age of AI and other data-intensive technologies

I. Introduction

The Centre for Information Policy Leadership[1] (CIPL) welcomes the opportunity to respond to the UK Government's call for evidence on *Data regulation in the age of AI and other data-intensive technologies*. For over two decades, CIPL has been a thought leader on data and privacy policy, law and implementation, championing organisational accountability and a risk-based approach as two key building blocks of modern regulatory approaches, responsible governance and use of data, including the accountable development and deployment of artificial intelligence (AI) and other transformative technologies.

CIPL strongly supports the pro-growth framing of this call for evidence and the Government's ambition for the UK to be the fastest-adopting AI economy in the G7. We have long argued that data is a valuable and too often under-valued asset, both in the public sector and the private sector. The task for regulation is therefore to enable the opportunity of data-driven innovation, prosperity and growth, while managing the risks proportionately and effectively and building continued digital trust.

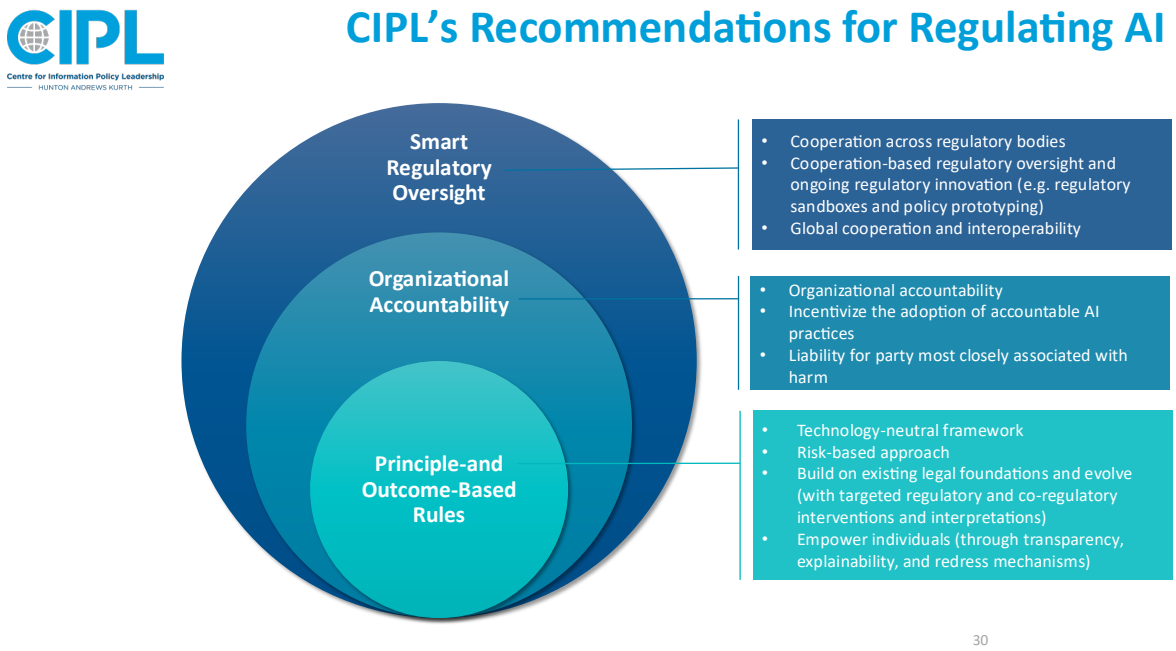
While AI presents certain risks and is well beyond the realm of data and privacy regulation solely, CIPL firmly believes there is risk in not developing innovative technologies and a risk of loss of opportunity. Regulatory uncertainty, compliance burden and legal friction create impediments for UK organisations, and reticence risks the loss of opportunity from not using and sharing data for the benefit of all. Taken together, these effects can weigh on the UK's competitiveness and on inward investment, and over time on its capacity to develop and retain data-driven industries.

This is not an argument for deregulation, nor for simply reducing the volume of rules. CIPL's position has consistently been that the UK needs a better and more proportionate policy

[1] **The Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank within the Hunton law firm that is financially supported by 85+ member companies that are leaders in key sectors of the global economy and by other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

framework, smart, effective and outcomes-based rules designed to achieve the best long-term results rather than to prescribe processes. While laws are necessary, no law is ever perfect or fully future-proof. Concepts such as demonstrable organisational accountability and other assurance models can be relied on to fill in the gaps and provide the necessary agility on the ground within the constraints of the principles and outcomes-based rules. This approach, coupled with smart and innovative regulatory oversight and behaviours that incentivise organisational accountability, must be the way for regulatory policy and approaches fit for the new digital world.

Graphic 1: CIPL's Approach for Regulating AI.[2]



This response is, in effect, a distillation of the positions CIPL has developed and advocated for over more than 25 years, and this call for evidence touches nearly every one of them. It also reflects the recent work of CIPL on simplification of digital rules, as distilled in our paper *Big Ideas for Simplification of Europe's Digital Rulebook.*

Rather than respond question by question, we structure our response around five big ideas that we believe should guide reform:

This response is structured around five big ideas for ensuring the UK's data protection and data framework is fit to enable responsible innovation, growth and sustainable digital trust.

[2] CIPL, Ten Recommendations for Global AI Regulation, 2023

1. **The GDPR: what worked, and the unintended consequences** — an assessment of the framework's real benefits and the areas where conservative interpretation, rather than the text itself, has held back responsible data use; a reflection on how the DUAA has begun to address this and where the reform could go further.
2. **Data protection does not operate in isolation** — how the tensions attributed to data protection often arise from its interaction with other rights, sectors and laws, and why reconciliation through holistic, interoperable policymaking is preferable to treating privacy in isolation.
3. **Tensions between data protection and AI** — the specific frictions between core data protection principles and how AI is built and used — purpose limitation, lawful basis, data minimisation, sensitive data, accuracy and fairness, allocation of responsibilities, transparency, individual rights —how each can be interpreted to enable responsible innovation and through mechanisms to preserve privacy such as PETs/PPTs.
4. **The evolution of regulatory development and oversight** — why the most effective response is not to have more prescriptive AI-specific rules, but to provide for an outcomes-based, risk-based framework, that encourages demonstrable and assured organisational accountability to fill the gaps the law cannot foresee and that equips regulators with modern, agile tools and discretion to prioritise action based on risks and growth, set strategic goals and invest in constructive engagement with and incentives for regulated entities.
5. **Future technological developments** — how the framework can remain fit for the new waves of disruptive and transformative technologies, from agentic AI to quantum, through a technology-neutral, accountability-based approach rather than a new regime for each wave of innovation.

We expand on each below.

II. The GDPR: what worked, and the unintended consequences

The GDPR set out to be principle-based, risk-based, technology-neutral and future-proof, serving not only data protection but "*economic and social progress*" (Recital 2) by aiding legitimate data use.[3] Measured against that ambition, CIPL assessed the effectiveness of the GDPR 6 years in and found that while the benefits have been real and lasting, the GDPR's full potential has been undercut – less by the text itself than by how it has been interpreted and applied.[4] The result is a set of unintended consequences that now weigh on responsible innovation. Most are fixable through interpretation; some need specific, laser-precise targeted legislative updates.

[3] Herke Kranenborg, About Profiles, Profiling, Data Availability and AI: The Return of the Second Objective of the GDPR?, 2025

[4] CIPL, GDPR Six Years On, 2024

What the GDPR got right:

- **Awareness and ownership**. It embedded data privacy awareness and accountability into organisations.
- **Privacy at board level**. Data protection became a genuine board and C-suite issue, with measurable return on investment from mature data and privacy management programmes.
- **A global baseline**. The GDPR became the de facto global standard (albeit more lightly interpreted and implemented around the world) that multinationals build their worldwide compliance and data management programmes around.
- **Organisational accountability**. It advanced accountability as an operational discipline – leadership, risk assessment, policies, transparency, training, monitoring and enforcement – shifting the burden of protection from individuals onto organisations.
- **Better data management**. It improved data hygiene, governance, traceability and breach resilience.
- **Transparency and trust**. It raised individuals' expectations of transparency and drove organisations to innovate in how they deliver it, strengthening trust.

Where it has fallen short – the unintended consequences:

- **Accountability and the risk-based approach were never fully realised**. Both are cornerstones of the GDPR, yet regulators have not consistently recognised or rewarded them. It is unclear that Data Protection Authorities (DPAs) apply the risk-based approach to their own priorities. Hence, high-risk practices are not always prioritised, and low- or no-risk technical breaches absorb attention. The incentive this creates rewards formal compliance over demonstrable, outcomes-focused accountability.
- **Conservative interpretation has restricted beneficial data use**. In CIPL's assessment, this is among the most significant constraints on responsible innovation. Regulators have tended to read the GDPR narrowly, focused on data protection in isolation from other rights and interests, contrary to the proportionate balancing the law envisaged. For example, narrow interpretations of the legitimate interest and contractual necessity legal bases for AI development have hindered responsible development, and now regulators globally are evolving their interpretations. This has led to the over-prioritisation of privacy versus other rights or obligations, such as fraud prevention, cyber security or physical and online safety, or even the rights and best interests of children.
- **Risk assessments lack clarity and consistency**. Organisations face uneven and often maximalist expectations around Data Protection Impact Assessments (DPIAs) and transfer risk assessments (TRAs/TIAs), creating unrealistic legal obligations, with little clarity that measures actually achieve anything in practice or are proportionate to actual risk.
- **The exercise of individual rights is not always proportionate in practice**. In a minority of cases, rights are exercised in ways that are disproportionate to any benefit to the individual concerned, including through the automated generation of high volumes of

requests. This imposes cost on organisations, and on regulators, without advancing the protective purpose the rights are designed to serve.

- **Certifications, codes of conduct and BCRs remain underused**. The GDPR created powerful co-regulatory tools to translate principles into practice. However, a lack of incentives to leverage these tools in practice, as well as complex, slow and inconsistent approval and administrative processes, have left this potential largely untapped. For example, there is no recognition that organisational accountability measures as per Article 24 GDPR are de facto the same as BCR requirements for a globally applicable privacy management program. There has also been limited appetite to date to explore the links between certification and data transfer mechanisms, such as BCRs and CBPR.
- **Oversight has favoured enforcement over engagement**. Constructive engagement, guidance and thought leadership have too often been crowded out, partly because enforcement is the most visible means of demonstrating impact, though not always the most effective, and partly because regulators are obliged to handle every complaint regardless of risk.
- **The framework is neither genuinely technology-neutral nor future-proof**. It has struggled to keep pace with new and emerging technologies, including generative AI or agentic AI.
- **The role of the DPO has become uncertain**. The GDPR elevated the DPO as the cornerstone of accountability, but the role's status and expectations have since become contested.
- **Complaint-handling and breach-notification burdens fall on regulators**. A duty to handle every complaint, and an over-strict reading of the 72-hour breach notification rule that drives defensive over-reporting, divert regulators from higher-value oversight.
- **Compliance costs and administrative burden have risen**. Prescriptive requirements have driven cost and paperwork beyond what is proportionate to risk, felt most acutely by smaller organisations and start-ups, which are among the most important sources of growth in the UK economy.

Amendments to the UK GDPR

The UK has reformed its data protection framework through successive legislative iterations, culminating in the Data (Use and Access) Act 2025 (DUAA). CIPL welcomes the changes introduced by the DUAA, but considers that the reform could have gone further. A number of sensible and proportionate measures proposed in earlier iterations of the reform were ultimately not carried forward. The table below sets out our position, identifying both the areas in which we are aligned with the reforms and those in which we consider more could have been achieved.

Table 1: Changes to the UK's data protection framework: where we are aligned and what could have gone further

Where CIPL agreed	What could have gone further

Scientific research (s.67–68). CIPL supports the new statutory definition of scientific research under the DUAA, to now include research carried out in commercial or for-profit contexts. This clear, flexible, consolidated definition reflects the reality that research is dynamic and increasingly AI-driven, and a narrow definition would exclude beneficial research.	N/a
Automated decision-making (s.80). CIPL supports the DUAA's move away from a prohibition on solely automated decision-making, now permitting such decisions in most circumstances that do not involve special category data, provided appropriate safeguards apply. This risk- and safeguards-based approach better reflects how automated decisions are actually used than an outright prohibition.	N/a
Legitimate interests – illustrative list (s.70). CIPL supports the new statutory list of activities that may amount to a legitimate interest – *including direct marketing, intra-group transmission for internal administration, and network and information security.* Bringing these examples into the text gives organisations greater certainty in relying on a basis CIPL has long viewed as a key enabler of responsible data use.	The list could have included AI training and model development, as it is often the most appropriate legal basis.[5]
Recognised legitimate interests (s.70). CIPL supports the new "*recognised legitimate interests*" basis, which removes the balancing-test requirement for a defined set of low-risk activities such as responding to emergencies, investigating crime, and safeguarding vulnerable people.	The list is confined to public-interest and security matters. CIPL has called for a broader whitelist covering routine, everyday business processing (e.g. payroll), so the balancing-test burden is lifted across the economy – not only for public-interest activities.[6]
ICO innovation and competition duty (s.91). CIPL supports the DUAA giving the ICO the power to have regard to innovation and competition, reinforced by a duty to consult other regulators on growth, innovation and	This remains a "have regard to" duty, subordinate to the protection objective, so its force depends on how actively it is used. The ICO's own pro-growth commitments – the experimentation regime, single AI

[5] CIPL, Legitimate Interests for AI Training: A DPO Perspective, 2025
[6] Ibid

competition, a published strategy and new performance reporting. Embedding these considerations in the regulator's remit is consistent with CIPL's long-standing call for smart and outcomes-based regulation.	rulebook and sandbox expansion[7] – go further than the statute requires, but rest on a voluntary letter rather than a firm footing, and were made under the outgoing governance model. CIPL would press for these to be operationalised and, where appropriate, placed on a firmer footing, and for the experimentation and sandbox approach to be cross-regulatory and cross-industry.
Purpose limitation (s.71). CIPL supports the DUAA's clarification of purpose limitation through a new Article 8A, setting out the factors for compatible further processing and confirming when re-use is permitted.	The purpose limitation principle could have been modernised to better support data processing within the AI lifecycle, where training is iterative and ongoing. CIPL would reframe further use in a risk-based way – focusing on safeguards, a new legal basis for secondary use of data, relevance and benefits, and impacts and rights, rather than a compatibility test.
Right to complain to the controller (s.103). CIPL supports the new right for individuals to complain directly to the controller, which must acknowledge the complaint within 30 days, take steps to respond, and inform the individual of the outcome. This is accountability in practice – resolving complaints at source, so regulators are not burdened with matters organisations can handle directly.	N/A
Data subject access requests (s.76, s.78). CIPL supports the DUAA placing on a statutory footing the "stop the clock" pause for obtaining identity or scope information, and the "reasonable and proportionate search" standard for access requests. Both give welcome certainty – though they largely codify existing ICO practice rather than introducing anything new.	The DPDI Bill's proposal to lower the refusal/charging threshold to "vexatious or excessive," aligning DSARs with the long-established FOIA standard, was not carried into the DUAA – retaining "manifestly unfounded or excessive." Adopting this could give clearer and more workable protection against disproportionate or manifestly excessive access requests.
DPIAs and RoPA retained. CIPL agrees that organisations must remain accountable for understanding the personal data they process – its uses, flows and sharing – and for	The DUAA could have evolved the DPIA and RoPA from their existing prescriptive form to being re-framed on an outcomes basis: requiring organisations to demonstrate that

[7] ICO, ICO response to government on economic growth, 2025

assessing the associated risks, benefits and impacts. That underlying accountability is essential and rightly survives the reform.	they understand their data, risks, benefits and flows and have assessed and mitigated impacts accordingly.
N/A	**Resolve tensions between data protection and AI**. The DUAA could have more explicitly reconciled the tensions between data protection law and AI development, for example data minimisation as a principle that does not restrict appropriate and proportionate data use if it is necessary for AI's development.[8]
N/A	**Outcomes-based senior data oversight role**. Reforms to the role of the DPO were ultimately dropped, but there is room to evolve the role by defining it by its outcome versus its tasks. Defining the role by outcome rather than by prescribed title would strengthen accountability while accommodating the range of governance models now in use.
N/A	**Incentives for accountability. Mitigating factor in enforcement**. The DUAA misses the opportunity to introduce incentives for organisations to embed accountability, including by treating a demonstrably implemented privacy management programme as a mitigating factor in decisions to investigate or enforce and in the assessment of penalties and fines, and by using demonstrated accountability as a "licence to operate" responsibly.

III. Tensions between data protection, AI and the wider digital framework

The consultation identifies a key theme which many practitioners have discussed for years – that data protection laws appear in tension with the technological development of AI. However, these perceived tensions may not arise from the framework itself, but in part from how data protection interacts with other rights, sectors and laws. As such, one way to ease these tensions is to reconcile the existing regime with the other rights and domains it sits alongside. In addition, it will be necessary to address the tensions themselves, either by evolving the interpretation of data protection principles, or by targeted changes to data protection rules.

[8] CIPL, Reconciling AI with the Data Minimisation Principle: Bridging the Innovation and Privacy Gap, 2025

Data protection does not operate in isolation

- No fundamental right is absolute, and data protection must be balanced against other fundamental rights and interests, including the freedom of expression and information, freedom from discrimination, and freedom of thought and autonomy. Upholding privacy in absolute terms and treating it in isolation can undermine other equally vital rights.
- There is not only a tension between privacy and other fundamental rights, but also a tension between data protection and other sections of digital regulation. Cyber security, the prevention of fraud and financial crime, online and offline safety, best interests of the children, and competition and interoperability frequently require and depend on using and sharing more data, not less – yet each is too readily framed as being in conflict with data protection. These different pillars of digital protection and regulation must be reconciled through holistic policymaking and interpretation, rather than by treating data protection as automatically prevailing over every other objective.
- The most effective response is to ensure any law is agile, principles-based and outcomes-focused, as well as supported by interoperable standards. Where tensions arise, frameworks should allow for agile and evolving interpretations that actually fit in with modern data-driven operations.
- Organisations should be encouraged to conduct holistic impact assessments to address different risks and benefits of use of data or deployment of new technologies, rather than be burdened to do isolated data privacy impact assessments, AI impact assessments, cyber security impact assessments, children's rights and online safety impact assessments.
- Fairness in data protection must be understood in relation to the underlying purpose and use of technology – not only if a data processing and use is fair to individuals and creates data protection risks for them, but also if not using data and not carrying out the intended purpose of processing is actually fair to individuals, groups of individuals and society at large.

Tensions between data protection principles and AI

Within this wider picture, the tensions between data protection and AI surface several core principles that must be resolved in order to ensure responsible AI development. The task is not to set these principles aside, but to interpret them in ways that enable responsible innovation while preserving the protection they aim to provide. Equally, if some principles need to be re-imagined and evolved to a different standard in the modern data and digital age, then some targeted changes of law would be required, too.

- *Purpose limitation* was introduced to prevent the indiscriminate re-use of personal data, but has been narrowly interpreted and now can be seen to sit in tension with AI development, which depends on data being reusable for beneficial and often

unforeseen purposes.[9] Indeed, the whole data society and economy will not only demand access to high value data, but also the re-use of existing data, powered by AI tools, which will place growing strain on purpose limitation as it is currently interpreted. The compatibility assessment can make re-use difficult even where new socially valuable purposes emerge after data collection. Model development should instead be understood as an iterative and ongoing process rather than a single, unrepeating stage; secondary data use for beneficial purposes should be permitted where it doesn't create new risks and harms for individuals (without the mitigations and corresponding benefits) and where it is supported by accountability-based safeguards rather than a rigid compatibility test.

- *Lawful basis.* Legitimate interests is often the only viable legal basis for AI training and development because of its flexibility, context balancing and built-in safeguards.[10] Consent is frequently neither feasible nor appropriate at the scale and speed of AI development.[11] Any data protection framework should explicitly recognise that legitimate interests is the legal basis for AI training and development, and recognise that it embeds additional accountability and controls by its very nature.
- *Data minimisation* should not be narrowly interpreted as using as little data as possible; it means using the data necessary for the processing. In the case of AI, this means enough data, including personal data, to ensure a well-functioning, accurate and demonstrably bias-mitigated system:[12] which often requires the AI to be trained for those purposes on large and diverse datasets. An overly restrictive interpretation can itself degrade fairness and accuracy – so data minimisation should be applied proportionately and in context, judged against the purpose rather than by volume alone.[13]
- *Sensitive data* is often needed to precisely detect and mitigate bias and ensure non-discrimination, yet the UK GDPR contains a blanket prohibition which prevents beneficial uses while doing little to reduce risk.[14] Organisations with limited or no access to processing sensitive personal data may struggle to test AI models appropriately for bias and discrimination, ultimately undermining fairness. The focus should shift from sensitive categories to sensitive uses, permitting processing that is necessary and proportionate under clear conditions and strong safeguards, and recognising lawful bases beyond consent, which is frequently impractical for large-scale AI development.
- *Accuracy and fairness.* The accuracy principle does not require model outputs to be correct in every instance; it concerns the accuracy of personal data relative to its purpose, and should be distinguished from the statistical accuracy of an AI system.

---

[9] CIPL, Response to the ICO's Second Consultation on Purpose Limitation in the Generative AI Lifecycle, 2024

[10] CIPL, Legitimate Interests for AI Training: A DPO Perspective, 2025

[11] CIPL, Response to the ICO Consultation on the Lawful Basis for Web Scraping to Train Generative AI Models, 2024

[12] CIPL, Reconciling AI with the Data Minimisation Principle: Bridging the Innovation and Privacy Gap, 2025

[13] CIPL, Applying Data Protection Principles to Generative AI: Practical Approaches for Organisations and Regulators, 2024

[14] CIPL, Rethinking Sensitive Data in the Age of AI, 2025

Representative, diverse data is a precondition of fairness, so requirements that restrict data or give effect to every erasure or objection could work against the very fairness and non-discrimination outcomes the framework seeks.[15]

- *Controller and processor* concepts do not map cleanly onto AI value chains, where responsibility for determining the purposes and means of processing is distributed and shifting.[16] As AI (and, increasingly, agentic AI) reshapes who decides what, an open question is whether these roles need to be reimagined, including whether a distinct form of responsibility should attach to those who develop the technology itself.
- *Transparency* should be meaningful and proportionate rather than maximal: it should give individuals the information they need in a layered, contextual and accessible way, without imposing disclosure that would undermine security, usability, or the rights of others.[17] The entity closest to the individual is generally best placed to provide it. Transparency is not only a regulatory safeguard but also an enabler of AI adoption: explainable and transparent AI systems are more likely to be taken up, which links directly to the Government's ambition to become the leading AI adopter in the G7.
- *Individual rights* must be applied with technical realism: rights such as erasure can be difficult or impossible to give full effect to once data is embedded in a trained model (similar to blockchain technologies), and may need clear boundaries where they would impose disproportionate burden or degrade model integrity. Furthermore, individual rights should not operate as a barrier to cyber security, the prevention of fraud, or the detection of sanctions breaches and money laundering. A targeted clarification or exemption in these contexts could support both public protection and trust.
- *International data flows* restrictions will impede the development of AI if data is confined to certain countries and lacks the representation, diversity and volumes that are required for AI development and deployment. Enabling data transfers based on a one-stop shop mechanism of demonstrable accountability, such as CBPR, BCR, and other assurance standards should be a priority for any government and its digital and industrial policy.
- *Definition of personal data.* Anonymisation and pseudonymisation should be assessed on a risk-based standard from the perspective of the data holder, recognising that the risk of re-identification need not be reduced to zero for data to be effectively anonymised, and rejecting an absolute, zero-risk threshold.[18]

In addition to evolving interpretations and targeted legislative changes, we need to invest in privacy-enhancing and privacy-preserving technologies (PETs and PPTs). Synthetic data, differential privacy, federated learning, homomorphic encryption, multiparty computational systems, and zero-knowledge proofs allow data to be used and shared across the AI lifecycle while remaining protected, and should be actively incentivised and given legal certainty, for

[15] CIPL, Legitimate Interests for AI Training: A DPO Perspective, 2025
[16] CIPL, Agentic AI White Paper, 2025
[17] CIPL Individual Rights Paper (incoming)
[18] CIPL, Big Ideas for Simplification, 2025

personal and non-personal (including confidential) data alike.[19] As such, Government should play a central role in investing in the development of PETs/PPTs, alongside empowering regulators to incentivise their use.

IV. Regulation and regulatory oversight

The consultation is seeking guidance as to whether an alternative regulatory approach might better suit AI – and where the current legal framework is working, where disproportionate barriers have arisen, and what should change. The most effective evolution is not more prescriptive, AI-specific rules, but a framework that is outcomes-based and risk-based, that fills the gaps the law cannot foresee with demonstrable accountability, and that equips both organisations and regulators with modern, agile tools.

- *Outcomes-based and risk-based regulation.* Regulation should focus on the results to be achieved rather than on compliance for its own sake, defining the outcomes organisations must deliver and holding them accountable for delivering them, rather than prescribing how compliance is documented or performed.[20] Results matter more than processes: an outcome-based obligation asks an organisation to understand its data and to assess and mitigate risk, not to complete a prescribed form, and this keeps the framework proportionate, future-proof and able to keep pace with technological change.
- *Regulatory leadership, guidance and prioritisation.* A regulator's responsibilities are numerous, and its resources finite, so clear strategic prioritisation is essential. The regulator's leadership function, and in particular clear, practical guidance that helps organisations get it right the first time, should take priority over a model built on deterrence and punishment: a results-based approach protects individuals in practice, makes the best use of scarce resources, and gives organisations the consistency and predictability they need to invest.[21] Government should enable this approach, including by empowering the regulator to prioritise the highest-risk harms through risk-based supervision.
- *Accountability as the mechanism that fills the gaps.* No law can anticipate every technology or use, so a principle-based framework must be given operational content through demonstrable organisational accountability.[22] The framework should recognise and reward it, through data protection management programmes, codes and certifications, and by treating it as a mitigating factor in enforcement, helping organisations that are seeking to get it right, while maintaining firm and proportionate enforcement against those that disregard the rules.

---

[19] CIPL, Understanding PETs and PPTs, 2023; CIPL, PETs and PPTs in AI, 2025

[20] CIPL, Getting the Best Outcomes: Pathways for Data Protection and Privacy Authorities, 2024

[21] Ibid

[22] CIPL, Building Accountable AI Programs: Mapping Emerging Best Practices to the CIPL Accountability Framework, 2024

- *Codes of conduct and certification.* The framework should make approved codes of conduct and certification schemes easier to establish and give them real weight as a route to demonstrating compliance. Just like accountability, these co-regulatory tools help organisations get it right and extend the reach of a resource-constrained regulator by reducing oversight and complaint-handling burdens, improving compliance through periodic re-certification, and building transparency and trust.
- *Regulatory sandboxes and experimentation.* Sandboxes let innovative uses of data be tested under supervision, and should be placed on a firm, well-resourced footing and made cross-regulatory and cross-industry – testing a whole sector's approach to a shared problem. Government should support the ICO's experimentation regime, including time-limited relief to test responsible innovation under supervision, with the findings feeding future guidance and reform.[23] Regulatory guidance and compliance should also be treated as iterative – something that can be tested and changed over time.
- *Public-sector data access and discoverability.* Government-held data can support innovation, public-service improvement and growth where it is made available securely, consistently and with appropriate safeguards. Future technological development depends on access to high-value public and private sector data, and government should enable and simplify this process.
- *Harmonisation of what good quality data looks like.* There is not yet a universally accepted definition of what constitutes high quality data. Government could consider harmonising the current approaches to what constitutes high-quality data into a single standard, which would afford organisations greater certainty in assessing quality, accuracy and suitability.
- *Operationalising the innovation and competition duty.* The framework already equips the regulator with an express duty to have regard to innovation and competition. Its value now depends on active operationalisation. Government should ensure the duty is given real effect, reflected in the regulator's strategy, priorities and reporting – and that the pro-growth commitments already made (the experimentation regime, single AI rulebook and sandbox expansion) are placed on a firmer footing that survives the transition to the Information Commission.
- *Empowering existing regulators over new prescriptive rules.* The most effective approach is to evolve the interpretation of the existing framework and empower existing regulators to apply it to AI, rather than layering on new, prescriptive AI-specific rules that risk fragmentation and quickly date.[24] Regulators should coordinate through cooperation bodies such as the world-leading Digital Regulation Cooperation Forum (DRCF) and work with other digital regulators in a more formalised way to limit fragmentation, with interoperability a guiding principle so that UK organisations are not caught between divergent regimes.
- *Balance between regulatory engagement and enforcement.* Modern digital regulators should be equipped, and expected, to prioritise on the basis of evidence of risk and

[23] ICO, Evolving regulatory sandboxes to meet the demands of AI and emerging tech, 2026
[24] CIPL, Ten Recommendations for Global AI Regulation, 2023

harm rather than on the visibility of individual cases. Constructive engagement, dialogue and cooperation with regulated entities should sit alongside enforcement as core regulatory tools, rather than below them. This approach incentivises good behaviours and good faith, favours transparency and dialogue and co-creative initiatives – from standards setting, to regulatory sandboxes and fast track processes. Enforcement should also be more creative with consent orders and mandating demonstrable accountability, similar to the US FTC consent decrees, for example, that actually create better outcomes and more embedded data management controls and safeguards in regulated organisations. Enforcement should be left for serious public interest cases of repeated or negligent breaches and disregard for the rules. Regulators must be driven by the purpose for which they have been established, their mission statements and realistic and relevant KPIs. Their success should not be measured principally by the number of enforcement actions taken or the value of fines levied, but by demonstrable improvements in outcomes for individuals.

V. Future technological developments

Beyond how data protection law applies to the technologies of today, the heart of this consultation asks whether the framework is fit to regulate the hugely disruptive technologies now arriving, from agentic AI to quantum. CIPL has long argued that technology-neutral, risk-based, principle-based frameworks, augmented by organisational accountability, are well placed to adapt to the technology as it evolves.

- *Risk-based approach to regulation, oversight and implementation as a driving force of the new approach.* Properly understood and implemented, risk based approach means three things a) legal rules and obligations must be based on risk of harm to individuals and society, considered together with benefits to individuals and society, b) organisations must be allowed to implement horizontal requirements on data and data protection through accountability based management programs in a risk based way, calibrating rules and compliance based on actual risk and benefits, and c) regulators must be required to set priorities and discharge their statutory functions, supervision, oversight, guidance-provision and enforcement in a risk-based manner. This model can be applied to regulation of any novel issues and technologies, too.
- *Agentic AI amplifies existing tensions rather than creating wholly new ones.* Agentic systems can self-initiate data collection, repurpose data and evolve their goals in real time, straining purpose limitation, data minimisation and the requirement for a clear legal basis. Consent becomes especially impractical where downstream processing is unforeseeable. Personalisation is likely to become a precondition of most agentic AI functionality, and something users come to expect as a matter of course — which in turn will require broader data access in order to deliver the service. Rigid interpretations of data protection principles would inhibit lawful, beneficial innovation; frameworks

should allow purposes to be defined broadly enough to accommodate reasonable evolution in an agent's functions, within people's reasonable expectations.[25]

- *The central novel risk is over-permissioning and delegated authority.* As agents act autonomously on behalf of individuals and organisations, the key new fault line is granting them more access than their task requires.[26] Guardrails on what personal data the agents can access, process and learn from, especially sensitive data, are essential.
- *Allocation of responsibility, transparency and rights become harder still.* Agentic value chains make it less clear which entity determines the purposes and means of processing and is therefore responsible for upholding individuals' rights, which the systems' autonomy can itself make harder to exercise. This reinforces the need to reimagine how controllership is understood as technology evolves.[27]
- *Emerging technology is also a privacy and compliance enabler, not only a risk.* Agentic AI can act as a first line of defence by limiting unnecessary human access to data, preventing over-collection. AI tools are increasingly used by organisations to automate, scale privacy, data management, cyber and AI compliance programmes. PETs and PPTs such as synthetic data, differential privacy and federated learning likewise allow data to be used and shared while remaining protected. These capabilities should be actively encouraged, as the consultation rightly recognises.[28]
- *The durable answer is an adaptable, accountability-based framework.* Because no law can anticipate the next technology, the framework's resilience depends on well-developed and incentivised accountability frameworks and a risk-based approach that scales governance to the likelihood and severity of harm; the roadmap organisations can rely on even in the absence of technology-specific guidance. Furthermore, UK digital regulators should be looking for ways to endorse good practices and demonstrable accountability, even agreeing on a uniform framework for demonstrating digital accountability across digital disciplines (privacy, cyber, safety, competition, children, etc). This is what allows the UK to remain fit for the future, accommodating agentic AI and whatever follows without a new prescriptive regime for each.

VI. CIPL's Big Ideas Paper

Set out below are the five themes for reform we identified in our Big Ideas for Simplification paper. We would welcome further discussion with the UK Government on how each might be applied in the UK context.

[25] CIPL, Agentic AI White Paper, 2025
[26] Ibid
[27] CIPL, Response to the DSIT Consultation on the Pro-Innovation Approach to AI Regulation, 2023
[28] CIPL, PETs and PPTs in AI, 2025

Centre for Information Policy Leadership
HUNTON

CIPL's Big Ideas for Simplification of Europe's Digital Rulebook

PART 1: SMART, SURGICAL UPDATES TO DATA PROTECTION LAWS

01
Modernise purpose limitation to enable responsible data reuse

02
Reimagine rules for sensitive data to unlock fair, responsible AI and data use

03
Update automated decision-making rules for the age of AI

04
Broaden research provisions to support public-interest innovation

05
Create a non-exhaustive list of recognised legitimate interests

06
Remove blanket cookie-consent rules and rely on the GDPR instead

07
Enable recognition of trusted international data frameworks including CBPR

PART 2: REMOVE FRICTION AND CONTRADICTIONS

01
Align privacy and safety duties with clear, proportionate rules

02
Align DMA and GDPR rules on consent to tackle consent fatigue

03
Align EU data mobility rules to support innovation and interoperability

04
Bring ePrivacy rules under the EDPB for consistent enforcement

05
Deliver digital fairness through existing laws, not new legislation

PART 3: COHERENT, TRUSTED DIGITAL ACCOUNTABILITY SYSTEM

01
Establish a common accountability framework across Europe's digital laws

02
Align GDPR and AI Act risk assessment requirements in law

03
Align user-facing transparency requirements across digital laws

04
Create a unified incident-reporting framework across digital laws

PART 4: EQUIP REGULATORS WITH MODERN, AGILE TOOLS

01
Make regulatory sandboxes a legal requirement

02
Require digital regulators to consider innovation, competition and growth

03
Enable risk-based supervision and enforcement for high-risk harms

04
Establish consistent consultation standards for digital regulators

05
Require cooperation and information sharing across digital regulators

PART 5: BUILD REGULATORY READINESS FOR CHANGE

01
Use GDPR margin of manoeuvre to enable practical, responsible innovation

02
Accelerate adoption of GDPR codes of conduct and certification schemes

03
Embed risk-based and outcomes-focused approaches across compliance

04
Establish and expand regulatory sandboxes across Europe

05
Advance transparent and evidence-based regulatory decision-making

06
Consolidate and extend coordination across Europe's digital regulators