CCIA Response to the DRCF 2027/28 Workplan Call for Input

CCIA welcomes the opportunity to respond to the DRCF's call for input on its 2027/28 workplan. CCIA is an international technology trade association representing a broad range of communications and technology firms. We have responded to several DRCF calls for input over the past two years, including on agentic AI, on consumer interest and AI, and on AI policy tools.[1]

Agentic AI is now the clearest case where overlapping remits between DRCF members might create unintended consequences. Members should coordinate in the coming year, before divergent approaches settle into unnecessary barriers to innovation.

All four members have set out how they intend to support growth and innovation, and the DRCF's own 2026/27 workplan records those commitments.[2] Where regimes meet, uncertainty about how they interact and how they will be enforced can deter legitimate improvements in digital services the rules are not intended to prevent.

1. Where we observe the greatest overlap

Agentic AI is an area where overlap is most pronounced, because a single deployment can engage consumer protection, data protection and, for services in scope, online safety at the same time.

The DRCF has already identified agentic AI as a cross-cutting question through its own call for views, and two of its members have since addressed the same technology within months of each other. In March 2026 the CMA published guidance for businesses using AI agents, which proceeds on the basis that existing consumer protection law applies and that the business deploying an agent remains responsible for what it does, including where a third party supplied it.[3] In October 2026 the ICO opened a call for evidence on agentic AI in which the allocation of controller and processor accountability across the development and deployment chain is among the live questions.[4]

Both approaches are coherent in their own terms. The difficulty for an organisation is that the same facts may produce different answers about which party in the chain is

[1] CCIA, Response to the DRCF Call for Views on Agentic AI, November 2025, https://ccianet.org/wp-content/uploads/2025/11/Agentic-AI-CCIA-Submission.pdf. CCIA, Response to the DRCF Call for Input on Consumer Interest and AI, July 2026, https://ccianet.org/wp-content/uploads/securepdfs/2026/07/DRCF-consumer-attitudes.pdf. CCIA, Response to the DRCF Call for Input on AI Policy Tools, August 2026, https://ccianet.org/wp-content/uploads/securepdfs/2026/08/DRCF-policy-tools-CCIA-response.pdf
[2] DRCF, 2026/27 Workplan, April 2026.
[3] Competition and Markets Authority, Complying With Consumer Law When Using AI Agents, March 2026, https://www.gov.uk/government/publications/complying-with-consumer-law-when-using-ai-agents
[4] ICO, Agentic AI Call for Evidence, October 2026, https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2026/10/agentic-ai-call-for-evidence/

answerable, depending on which regime is applied. An organisation deploying an agent built on a third party model needs to know whether it is expected to account only for what it determines, or also for upstream processing it does not control and cannot observe. That question is being approached by two regulators at once and the answers have not been reconciled.

The labels each regime uses add a further layer of difficulty. "Developer", "deployer" and "provider" are used in AI and consumer contexts, "controller" and "processor" in data protection, and "trader" in consumer law. A single organisation can be described with different labels under each regime for one deployment, and the labels do not map onto each other cleanly.

Survey research conducted for CCIA by Freshwater Strategy and published in October 2026 found that 62% of UK technology businesses consider uncertainty about enforcement a bigger issue than the rules themselves, and that 52% have been prevented from undertaking a business activity as a result. 28% report avoiding beneficial uses of data where it was unclear whether they were permitted. The same research finds that if the burden were eased, 68% would use data more extensively and 62% would adopt new data or AI technologies.[5] Uncertainty at the boundaries between regimes is what the DRCF is placed to reduce, and doing so is the most direct contribution coordination can make to growth.

A second and more specific friction concerns logging and retention. Accountability in agentic systems is commonly evidenced through logs recording which agent acted, under what authority, and what information it accessed. Those logs frequently contain personal data. An expectation of comprehensive logging in the service of accountability therefore sits in tension with data minimisation and storage limitation, and with record-keeping expectations elsewhere that may point to different retention periods. This is a current and practical problem, and it arises precisely at the intersection of two members' remits.

Age assurance raises a similar tension between Ofcom and the ICO. Establishing age to the standard the online safety regime expects can involve processing sensitive personal data, while the data protection regime expects collection to be kept to a minimum. Where checks are repeated service by service, the same person may end up providing that data to many separate organisations. A joint view on what proportionate age assurance looks like across both regimes, which remains open to a range of technical approaches rather than favouring any one, would help services meet both sets of expectations.

2. Opportunities for joint action

AI regulation is not a single field. In practice it addresses a range of priorities that already sit with existing regulators, including data protection, consumer protection, financial stability and online safety, alongside emerging opportunities and risks that do not yet sit cleanly with any of them. No single regulator can address all of that, and an attempt to

[5]Freshwater Strategy for CCIA, UK Data Regulation Survey, October 2026, https://ccianet.org/research/stats/freshwater-strategy-uk-data-regulation-survey

create one would risk duplicating work already being done, cutting across the domain expertise that makes the existing regulators effective, or both.

AI innovation therefore also has the potential to face a particularly onerous cumulative regulatory burden. Without some measure of coordination, innovation could be undermined to a greater degree than would be considered proportionate by any individual regulator.

A productive role, and one similar to what the DRCF already performs, is that of a clearing house: a forum in which emerging regulatory opportunities and threats are discussed with bodies holding relevant technical expertise, including the AI Security Institute and the National Cyber Security Centre, and with the firms building and deploying these systems, and then worked through into what they mean for the functions of existing members. Sustained working relationships with AI expertise in industry would give that function a foundation in how the technology is actually built and used, rather than in how it is described after the event.

Lead regulator designation. Where a single agentic deployment engages two or more members, there would be value in a mechanism for identifying which regulator leads, with the others working through that lead rather than in parallel. The positive impact would be greater regulatory certainty, a single point of engagement, and less duplicative reporting of the same incident to several regulators. This limits the potential for a tragedy of the anticommons where multiple regulators can hold up innovation and none can give a clear go ahead.

A shared statement on terminology. A short cross-regulator note mapping the terms used across the regimes, and identifying where the same word carries different meanings, would be inexpensive to produce and would remove a recurring source of confusion. This is an output the DRCF is well placed to deliver and that no individual regulator can.

Sequencing of guidance on shared technologies. Where two or more members are preparing guidance touching the same technology, a joint statement on how the regimes interact, published before or alongside the individual guidance, would spare organisations having to reconcile the documents afterwards. Agentic AI is the immediate candidate.

Reconciling accountability with data minimisation. A joint position on what logging and retention is proportionate for agentic systems, developed between the ICO and the members whose regimes impose record-keeping duties, would resolve a tension that organisations currently manage by judgement alone.

An optional coordinated route before launch. Building on the Thematic Innovation Hub, firms bringing products that engage more than one regime could put a single set of questions to the relevant regulators and receive coordinated early feedback. This should remain voluntary and support, rather than replace, each regulator's own decisions. Publishing which regulators take part, indicative timescales and the status of any advice would make it more useful to smaller firms in particular.

Understanding cumulative burdens on innovation. The DRCF is well placed to bring together analysis of the regulatory costs being created for AI innovation, how that cumulative burden might affect development and deployment of new AI-enabled services

and where there might be opportunities to address that issue by working across regulators or with emerging international industry standards.

3. Risks that regulators should address together

Divergent allocation of responsibility in agentic AI supply chains, spanning the CMA and the ICO. Neither regulator has taken an unreasonable position, but organisations are left facing inconsistent expectations about which party answers for a system's behaviour. The cost falls on UK deployment, because an organisation that cannot determine its exposure will tend to limit what it offers here. It is not a problem either can fix on its own.

Authorisation and redress where agents act across services, spanning the ICO, the CMA and the FCA. When an agent acts on a person's behalf across third-party services, it is not yet clear how authorisation should be evidenced or where a person should go if something goes wrong. A shared view on those questions would give consumers confidence and firms a clear basis for designing these services.

Scams involving AI agents, spanning Ofcom, the CMA and the FCA. Fraud that uses agents to initiate or complete payments cuts across online safety, consumer protection and financial services. Coordinated work here would help close gaps between regimes and spare firms inconsistent expectations from each.

Accountability logging against data minimisation, spanning the ICO with Ofcom and the FCA. Expectations that agent activity be comprehensively logged for accountability purposes run against data protection principles and against differing record-keeping requirements elsewhere. The risk is that organisations are exposed under one regime for doing what another appears to require.

Age assurance and data minimisation, spanning the ICO and Ofcom. This is already in train under the DRCF 2026/27 workplan and we support its continuation.

CCIA would welcome the opportunity to discuss any of the above. We are happy for this response to be published.