The Council Has Given the Digital Omnibus a Workable Direction – At Least

The agreed mandate would make useful data processing more predictable. Losing these reforms would preserve uncertainty that Europe can ill afford

Dr M.R. Leiser (Mark)
DigiData Consulting Ltd · 22 October 2026

This article builds on The Unfinished Rescue, The Entrenchment Move, Context Is Not Fragmentation, Regulating the Regulator and The Innovation Mandate. My research critiques, When "Scientific Research" Stops Being Scientific and One Bad EDPB Joint Opinion Spoils the Apple, explain the need for legislative correction.

The anonymisation series develops the alternative: Anonymisation After SRB, Context Is Not a Loophole, Anonymisation, Two Ways, The Missing Route to Lawful Use, The Omnibus Must Build the Road, Non-Personal Data Is Not One Thing and Anonymous Enough to Share, Personal Enough to Police?. Europe Will Not Build a PET Market on Legal Ambiguity, The September Test and The Trouble With noyb's Cookie Banner Campaign connect those arguments to practical reform.

My legal certainty report sets out the detailed proposals.

The official mandate, ST 14756/26, published on 22 October, sets out the position agreed on 21 October. The four models below explain that agreed text. Parliament still awaits a committee decision; the Council's mandate establishes a negotiating position, not new law.

Identifiability Must Follow Actual Capabilities

Well done to the Council. Its Digital Omnibus mandate recognises that legal certainty serves the people whom data protection law protects. Patients benefit from workable research collaboration. Users benefit when developers can test systems against representative data. Organisations have a stronger reason to invest in privacy engineering when effective safeguards produce a dependable legal consequence. The Council has looked beyond the scaremongering that treats any recalibration as an assault on rights.

The Council preserves Article 4(1)'s definition and places its recipient rule in Article 25a. The resulting architecture recognises that effective separation can alter an independent recipient's legal position while preserving responsibility for the original controller, its processors, and identifying onward disclosures.

Model 1: Recipient Status Under Proposed Article 25a

Actor	Relevant capability or relationship	Result under the mandate
Original controller	Retains the key or another realistic identification route.	The data remain personal for that controller.
Independent third party	Cannot identify through means reasonably likely to be used.	The pseudonymised data are non-personal for that recipient.

Actor	Relevant capability or relationship	Result under the mandate
Processor	Processes personal data on behalf of the controller, even without the key.	The data remain personal for the processor.
Onward disclosure	A third party makes the data available to a further recipient with reasonably likely identification means.	Both that transmission and the further recipient's processing involve personal data.

Assess all reasonably likely means of direct or indirect identification. A missing name alone does not establish non-identifiability.

A hospital retaining the key to coded records still processes personal data. An independent research recipient may reach a different classification if its actual capabilities and realistic access routes leave identification insignificant in practice. A processor acting for the hospital cannot claim the same consequence simply because the hospital withholds the key. Nor can a recipient pass the records to an identifying third party while disregarding the legal character of that transmission.

The rule therefore rewards a demonstrable change in capability. A contract can contribute to effective separation, but its wording cannot eliminate a realistic linkage route. Persistent advertising identifiers also require scrutiny: recognition across encounters and individual targeting may establish identifiability without revealing a civil name. The Council's recital 27b expressly includes singling out and online identifiers in the assessment.

The gain is practical. A researcher or PET supplier can point to an operative provision when explaining why a carefully bounded arrangement changes the recipient's obligations. EDPS v SRB already rejects automatic personal-data status for every recipient of pseudonymised information. Losing Article 25a would therefore leave that case law intact.

It would also leave organisations to reconstruct the compliance consequences through opinions and disputes, with less dependable grounds for investment. Smaller participants bear that uncertainty particularly badly because they cannot spread bespoke legal costs across hundreds of deployments.

AI Development Needs Predictable Permission

Article 88 bis makes a legitimate-interest route explicit while retaining Article 6(1)(f). That combination deserves support. A legislature can recognise that an activity may pursue legitimate interests without deciding whether a particular operation satisfies necessity and balancing.

Model 2: AI Processing Still Requires the Article 6 Assessment

Question	What the controller must establish
Legitimate interest	Identify a lawful, real and sufficiently specific underlying purpose. AI development alone does not supply that purpose.
Necessity	Show why the processing is necessary for that purpose, considering less intrusive means that would work as effectively.
Balancing	Establish that the data subject's interests or fundamental rights and freedoms do not override the interest pursued.

Question	What the controller must establish
Additional requirements	Apply the other GDPR duties and relevant safeguards. Sensitive data require a separate Article 9 condition; Article 21 operates on its own terms.

The first three conditions remain cumulative. Article 88 bis expressly accommodates this route; it does not approve every AI operation.

Pablo Trigo Kramcsák and Lorenzo Dalla Corte argue in European Law Blog that express recognition could influence the assessments that follow. Of course, legislation influences legal assessment. The question is whether the provision excuses controllers from substantiating their processing. Article 88 bis does not remove the cumulative conditions of Article 6(1)(f), and recital 33a expressly rejects AI development as a legitimate interest in itself.

Parliament should put that qualification in the operative provision, alongside clearer conditions for reliance.

A developer testing a language model across regional dialects must identify the purpose of its work, explain the proposed data's contribution, and consider effective, less intrusive alternatives. It must assess the effects on the people represented. An express legislative route lets that assessment begin from a clearer position on available grounds. It should also constrain attempts to make consent the practical default merely because the project uses AI or pursues a commercial aim.

Europe gains a better basis for responsible access to data, including the evidence needed to detect uneven performance. If the clause disappears, AI training does not suddenly become unlawful. Developers instead lose the certainty that express recognition in the GDPR could provide and remain more dependent on the interpretation and application of a general provision.

The likely opportunity cost is that projects are narrowed, delayed, or abandoned before anyone tests whether appropriate safeguards would permit them.

Article 9 still requires a separate justification. The Council's narrow exception for unintended, incidental residual sensitive data addresses a genuine technical problem without authorising deliberate sensitive profiling. Responsible development requires workable duties to avoid collection, erase material, and, where erasure is technically impossible or manifestly disproportionate, effectively prevent further processing and disclosure.

Demanding a result that technical systems cannot achieve does not replace those enforceable duties.

Research Must Qualify on Its Merits

The Council's research definition expressly accommodates commercial aims in the operative text. Recital 28 also recognises company mandates and legitimate confidentiality. Those choices correct the tendency to judge research through the institutional arrangements familiar to academic researchers.

Model 3: Scientific Research Follows Substantive Criteria

Element	Requirement or clarification in the Council text
Purpose and knowledge	Aim to contribute to society's general knowledge and wellbeing; generate new or complement existing scientific knowledge.

Element	Requirement or clarification in the Council text
Method	Use a methodological, systematic approach consistent with the relevant field's standards, including ethical standards.
Results and independence	Produce verifiable, transparent results in an autonomous and independent manner.
Commercial aim	Research may also further a commercial interest. Profit neither establishes nor defeats scientific character.
Interpretive safeguards	Recital 28 accommodates company mandates and legitimate limits on public access, including intellectual property and trade secrets.

The operative criteria work together. Scientific status does not itself provide a lawful ground or displace the safeguards in Article 9 and Article 89.

The EDPB's April consultation draft permits commercial research. My criticism concerns its presumption: projects meeting all six indicative factors qualify presumptively, while others must justify their scientific character. The treatment of qualifications and institutional examples risks making conventional academic arrangements the easiest route through that assessment.

The February Joint Opinion compounded the problem by recommending that legislators move the commercial-interest clarification into a recital.

A medical technology company investigating a measurement failure can generate scientific knowledge through rigorous methods. Practical expertise may equip its researchers for the work; patent protection may justify delayed publication. A university affiliation does not establish scientific integrity, and a commercial sponsor does not disprove it. Keeping the clarification in the definition gives controllers a firmer basis for resisting that institutional bias.

The benefit would extend to cross-border collaboration through a common statutory starting point. Failure would preserve the existing scope for commercial research, but forgo clearer legislative protection against restrictive interpretations. The Council has not solved every problem: national Article 9 differences remain, and a rigid reading of independence or transparency could turn the definition's criteria into new barriers.

Parliament must protect methodological integrity without demanding institutional detachment or unrestricted publication. Otherwise, reform could reproduce the assumptions it should correct.

Cookie Reform Should Reward Less Intrusive Design

The Council keeps device-access rules in ePrivacy and draws additional purpose-bound exceptions. That choice respects the independent device-access trigger while recognising that constrained measurement differs from constructing behavioural histories across services. Anonymity for a recipient cannot, by itself, establish an ePrivacy exemption.

Model 4: Selected Cookie Permissions and Their Limits

Operation	Principal conditions for the proposed exception
Own-service audience measurement	Create anonymous aggregates through the provider or someone acting on its behalf. No other-purpose use, third-party sharing or combination with third-party data.
Media audience measurement	Comply with EMFA Article 24; pseudonymise after collection; avoid other-purpose use and tracking beyond the service or content. Sharing outside the permitted provider arrangement must contain no personal data.
Contextual-ad performance measurement	The ad uses immediate visit content or a single query and involves no personal-data processing. Provider-led measurement must avoid profiling and past or future behaviour; pseudonymise after collection and prohibit reuse.
Operation fails every listed exception	Obtain valid consent for device storage or access. Any associated personal-data processing must also satisfy applicable law.

Selected exceptions only. The mandate requires sole connection and strict necessity to a listed purpose. A recipient's lack of identifiability does not, by itself, exempt device access.

The gain lies in incentives. A publisher that limits collection and reuse should have a dependable reason to prefer a constrained measurement system. If every technically useful operation produces the same demand for consent, regardless of its architecture, the law weakens the incentive to choose a less intrusive design. Repeated demands also compete for the attention users need when their choices have greater consequences.

The agreed text couples its exceptions with an easy single-click refusal and a minimum four-month interval before another request for the same purpose after refusal. These rules give the reform a direct benefit to consumers. If the exceptions fail, the cost will include continued demands for permission in cases where legislators could instead prescribe bounded conduct. That outcome would preserve friction without establishing that the friction produces corresponding protection.

Parts of the anti-AdTech debate have become good at putting "dignity", "autonomy", and "control" in the opening paragraph, then leaving the difficult design choices to someone else. Those concepts deserve rules specifying who must do what and how people can challenge misuse. Repeating "control" will not tell a publisher how to measure an audience without building a tracking business. A workable rule should follow the rhetoric more often.

Automated privacy signals do offer a concrete mechanism. I continue to support reusable choices, with clear legal effects and safeguards against browser gatekeeping. The Council's removal of that scheme leaves work unfinished. Its contextual-advertising provision also needs a clearer distinction between ad selection without personal-data processing and the measurement data that providers must pseudonymise. Parliament should resolve that ambiguity while preserving the purpose-bound approach.

The Mandate Should Go Further

The cost of failure would fall across this package through a familiar pattern: useful activity would depend more heavily on an organisation's ability to finance uncertainty. Existing lawful routes would

survive, but smaller researchers and developers would lose an opportunity for more predictable permission. Europe would also weaken the case for investing in safeguards whose legal consequences remain difficult to establish in advance.

My preferred settlement goes beyond the mandate. The GDPR should express contextual, actor-relative identifiability as a general rule, with explicit protection against artificial separation, collusion and foreseeable identifying onward transfers. Article 25a supplies a useful application of that principle; it should not leave the general boundary dependent on the technique a controller selects.

Legislation should then attach a rebuttable basis for reliance to documented assessments using approved methods and independent assurance. Concealed access routes, deliberate reidentification and material changes in capability would defeat reliance. That system would give effective privacy engineering a predictable return while preserving an authority's ability to challenge an assessment with evidence.

For AI and research, the next step is a clearer statutory route to safeguarded data use. Parliament should preserve Article 6(1)(f)'s assessment while making the permission and conditions sufficiently precise to support investment. Research provisions should exclude institutional gatekeeping and establish common minimum safeguards. Cookie reform should combine bounded exceptions with usable, portable preferences whose legal effects the legislation defines.

Finally, the EDPB and EDPS need a duty to cooperate across overlapping regimes and a bounded Innovation Mandate. When authorities exercise market-shaping discretion, they should identify the risk, compare lawful alternatives and explain the consequences for legal certainty and European innovation. That duty would discipline discretion within the law; it would neither create a legal basis nor override a prohibition.

The next stage should turn this mandate into a more ambitious settlement, starting with statutory assurance of recipient-relative identifiability and an Innovation Mandate requiring supervisors to explain how responsible innovation can proceed.

First published on DigiData on 22 October 2026.