The Digital Omnibus Has Reached Its September Test

Why legal certainty, the GDPR's personal-data trigger and a disciplined supervisory state belong in the same reform conversation

Dr M.R. Leiser (Mark)
DigiData Consulting Ltd · 8 September 2026

The Council's 11 September discussion will test whether Europe's digital rules can become more predictable, improve cooperation between authorities, and reward demonstrable reductions in risk.

This week at a glance:

Thursday: ITRE meets, but the Digital Omnibus is not on its published agenda.

Friday, 10.00 Brussels time: the Antici Group (Simplification) examines the restricted Presidency package.

On Friday 11 September, at 10.00 Brussels time, the Council's Antici Group on Simplification will meet in the Justus Lipsius building. Its sole substantive item is the Digital Omnibus. Member State representatives will exchange views on a revised Presidency compromise, ST 12535/26, and a steering and explanatory note, WK 13065/26. Both texts exist, both are marked LIMITE, and neither is publicly available.

The meeting prepares the Council's position; it does not constitute a ministerial vote, a general approach or the opening of trilogue negotiations.

The rest of the week is quieter. Parliament's ITRE committee meets on Thursday, but the published agenda does not include this file. Parliament still records the procedure as awaiting committee decision; its June draft report and July amendments have not yet become a committee position or negotiating mandate. The Council is therefore moving first, under conditions in which the public can see the questions but not the latest answers.

Friday's exchange will probably test support, expose remaining fault lines and shape the next Presidency draft. Nobody outside the negotiating circle can responsibly claim that the restricted text has solved the definition of personal data, AI development or public-sector data. What we can say is that this week offers a live drafting opportunity.

Co-legislators can choose whether essential legal rules sit in the GDPR's operative text, or whether uncertainty returns in another form through recitals, implementing acts, and supervisory guidance.

Simplification Means Legal Certainty

The Commission proposal presents the Digital Omnibus as targeted simplification: clearer rules, lower compliance costs, stronger competitiveness and continued protection of fundamental rights. That objective reflects the wider Commission simplification agenda, which recognises that cumulative regulation can impose costs far beyond the value of any single reporting or compliance rule.

But simplification is not measured by deleted articles. Removing an operative rule does not help if a university, scale-up or public body must reconstruct the answer from judgments, non-binding

guidance, national practice and litigation. Delegating a central question to the EDPB instead moves a political choice into a form that is harder to rely upon, challenge and keep stable.

The July Presidency note identified the pressure points: identifiability, pseudonymisation, AI development, residual special-category data and the division of responsibility between legislators and the EDPB. Legislation must settle the perimeter, consequence and burden of proof; expert bodies can keep technical methods current within it. Legal certainty tells people which rule applies, which evidence supports the assessment, which safeguards change the result and who may decide.

Personal Data: For Whom?

The definition of personal data in Article 4(1) GDPR is the gateway to the Regulation. It determines when the GDPR applies and when it overlays the AI Act, Data Act, research infrastructures, health data spaces and ePrivacy rules. An overextended trigger can keep pseudonymised information concentrated inside the organisation holding the key, even where an independent recipient has no realistic means of identification.

The Court's judgment in EDPS v SRB supplies the doctrinal starting point. The Single Resolution Board sent coded comments to Deloitte while retaining reconnecting information. The Court rejected the idea that pseudonymised information must be personal data in every case and for every recipient. Identifiability depends on the means reasonably likely to be used by the relevant actor in the real legal, technical and organisational setting.

The assessment must account for cost, time, labour, technology and lawful access routes. Information may remain personal for the body holding the key while falling outside the definition for an independent recipient whose identification capabilities face effective constraints.

That actor-relative approach is not a loophole. A group cannot split functions artificially, place the key with an affiliate, procure identification through a processor or arrange a foreseeable onward transfer and then rely on the immediate recipient's lack of names. The factual question is who can realistically identify, by what route, for whose purposes and at what point.

The EDPB's July EDPB anonymisation guidelines acknowledge that anonymity may vary between entities and that theoretical possibility is insufficient where identification is insignificant in reality. Yet guidance cannot itself provide a stable reliance rule, and imaginary future recipients or a generic malicious actor will still overclassify data. The legislature must make contextual identifiability documentable, auditable and trustworthy.

The Third Route

My Digital Omnibus report develops a third route between two unsatisfactory positions. The Commission recognised the certainty problem, but its Article 4 amendment needed stronger anti-circumvention safeguards, and the proposed Article 41a gave implementing acts too much scope-changing power.

The EDPB and EDPS Joint Opinion and last public Council compromise move too far the other way by returning decisive questions to Article 29a, supervisory interpretation and litigation. That protects discretion, not certainty. I set out the wider argument in The Omnibus Must Build the Road.

The third route combines legislative contextuality, operational safeguards, usable assurance and institutional discipline.

Legislative contextuality means applying an ex-ante, in concreto, actor-relative test in Article 4. The entity should assess its actual capabilities, realistic access to auxiliary information, cooperation with others, foreseeable transfers and current technology. Metaphysical possibility is not identifiability. The claimant should document why identification is insignificant in practice; an authority disputing that conclusion should identify a realistic route that defeats it.

Operational safeguards prevent evasion. The GDPR should apply where an actor can procure identification, a processor or affiliate acts for it, corporate separation is artificial, effective access to the key remains, or an identifying transfer is designed, known or foreseeable. Material changes in capability, auxiliary data or recipient should trigger reassessment.

Usable assurance gives privacy engineering a legal return. Article 29a should establish a documented assessment covering actors, purposes, access, isolation, linkage, controls, onward circulation and time. Approved methods, codes or independent certification should create a rebuttable presumption of reasonableness at the assessment date. Concealed facts, collusion, deliberate reidentification or material change would defeat reliance.

Pseudonymisation and privacy-enhancing technologies should purchase a predictable regulatory dividend, not cost money without changing the legal result.

Institutional discipline completes the design. The legislature sets the trigger, burden, guardrails and consequence. The EDPB maintains methods, attack models and reassessment criteria. Authorities enforce and courts review. Technical standards remain current without letting guidance shift the legal threshold by stealth.

AI Needs Data, and the GDPR Should Say So

The AI question starts from a straightforward premise: Europe needs substantially more data for AI development. The Data Union Strategy makes access a competitiveness priority, while the Commission's Digital Package FAQ promises high-quality and fresh datasets, including data labs for companies, researchers and smaller firms.

Data scarcity and uncertain permission favour incumbents with proprietary corpora, legal teams and capacity to absorb enforcement risk.

More data is good for AI when it is relevant, diverse, representative and governed. Scale alone will not cure poor curation or historic bias, but artificial scarcity is no answer. The Chinchilla study showed the performance value of much more training data under a fixed compute budget. The WILDS benchmark records failures across hospitals, countries, time periods and groups when systems face distribution shifts.

NIST bias guidance explains why representative data and sometimes group information are needed to find systematic error. The AI Act itself requires representative training, validation and test data covering relevant settings. Data protection law should enable the data conditions that AI safety law demands.

The Commission chose the right institutional form in proposed Article 88c: the rule belongs in the GDPR's operative text. But it stopped short of solving access. Necessary processing for AI may be pursued as a legitimate interest, yet every developer returns to necessity and balancing. The June Council approach went backwards into recital 33a, where AI development may qualify only in certain cases.

The EDPB AI opinion and joint institutional position leave the result project-specific. The Omnibus should remove that uncertainty.

Article 88c should provide affirmative, predictable permission to acquire and use lawfully accessible personal data to develop, train, test, validate, evaluate and improve AI. Lawfully accessible preserves copyright, confidentiality, trade-secret, security and sectoral limits. Within data protection law, however, developers should not relitigate dataset legitimacy by dataset, authority by authority, and Member State by Member State.

Safeguards should target concrete harms, not data volume. Developers should prevent unlawful disclosure, deliberate reidentification, memorisation of identifying material, harmful outputs and repurposing that breaks access conditions. They should maintain provenance and security, test for leakage and bias, and use pseudonymisation, secure environments and privacy-enhancing technologies where these reduce risk without destroying utility.

Those controls should make access easier and more certain, not become a disguised permission process.

Special-category data require the same functional thinking. Sensitive attributes can be necessary to detect bias and avoid statistical blindness. The 2026 AI Act amendment permits exceptional processing where strictly necessary for bias detection and correction under strong safeguards. The Omnibus should align Article 9 and deal sensibly with residual or incidental sensitive data in large corpora.

Protection can require access: unequal performance cannot be tested across groups the developer is forbidden to observe.

This is not deregulation but a clearer exchange. Legislation grants usable access for socially and economically important development. Developers accept duties aimed at misuse and harmful effects; regulators enforce them and courts review them. The present model controls possibility at the input stage while leaving access uncertain, slowing European development without guaranteeing safer systems.

Public Access Must Remain Open

The public-sector data provisions pose the same question. Folding the Open Data Directive into the Data Act could improve coherence. Proposed Article 32r(4), however, would let public bodies impose special reuse conditions on very large enterprises, while Article 32q(6) already permits proportionately higher charges. The first fragments permission; the second can recover exceptional costs without breaking the open-data commons.

Charging and licensing are different. A public body can charge an intensive commercial user for an API or bulk service while leaving downstream rights intact. An actor-specific licence follows the data, forcing repositories, research consortia and smaller firms to trace provenance, user status and recipients across combined datasets. Incumbents can fund clearance. Smaller European innovators often cannot. A rule aimed at large firms can therefore entrench them.

Parliament has a credible cross-party route out. Amendments 831 to 834 would delete Article 32r(4); EPP amendment 835 would confine differentiation to charging. See the Parliament amendments and COMMUNIA analysis. These are tabled proposals, not Parliament's position, but the common insight is right: retain proportionate charges where justified and preserve open, interoperable public-sector licences.

Open licensing is part of Europe's AI strategy. Researchers and new entrants need permission that survives combination, collaboration and downstream use. Europe should make publicly financed data usable under common terms, particularly for research and smaller innovators, rather than recreate a legal toll booth at every transfer.

A Duty to Cooperate for the EDPB and EDPS

Clearer legislation still operates inside a crowded supervisory state. The same model, platform practice or data-sharing arrangement can engage privacy, AI, competition, consumer, cybersecurity and data-access law. Personal data gives privacy authorities a relevant voice, not authority to settle the whole answer unilaterally.

My Duty to Cooperate paper proposes a binding horizontal duty for the EDPB, EDPS, national data protection authorities and their counterparts where mandates overlap. It should require notice, lawful exchange, timed consultation, confidentiality and defence rights, reasoned divergence and coordinated remedies, with auditable separation between the EDPS's secretariat, advisory, supervisory and AI roles.

Cooperation is not consensus or a mega-regulator. It should not redistribute competence, create a veto or let silence stall urgent lawful action. Review should address serious failures that can affect outcomes, defence rights, competence conflicts, or remedies. The EDPB cooperation template and Meta Platforms v Bundeskartellamt point to coordinated administration, but neither provides a complete horizontal duty.

The simplification link is direct. Organisations experience overlapping requests, inconsistent definitions, duplicated evidence and remedies pulling in different directions. A Duty to Cooperate reduces institutional uncertainty without weakening any substantive mandate.

The Innovation Mandate

The Innovation Mandate supplies the broader governing principle. The third route determines what the Digital Omnibus should enact. The Duty to Cooperate governs how authorities should interact. The Innovation Mandate governs how a supervisor should choose between materially different courses that Union law already permits.

It should be a binding secondary duty for general and market-shaping discretion. For major guidance, priorities, sandbox criteria, consistency positions or remedies, a supervisor should identify the risk, disclose evidence and assumptions, compare rights-preserving alternatives, assess legal certainty, SMEs, investment, cross-border scale and adjacent regimes, and explain proportionality. A supervisory impact statement and public evidence register would expose that discipline.

The Mandate cannot reopen a prohibition, create a legal basis, weaken protection for vulnerable people or let outsiders direct an individual case. It operates within the lawful choice set. Within that space, innovation, investment and European scale are legitimate public interests, and supervisors should show that they considered them.

That is why affirmative AI data access belongs in legislation. The Innovation Mandate can discipline supervisory choices but cannot cure an unresolved permission. Parliament and Council must decide that Europe wants researchers, start-ups and established developers to have the data needed to build and test capable systems. The EDPB and EDPS should administer that choice coherently with other authorities.

Friday's discussion is about more than drafting. The Council should codify contextual, actor-relative identifiability; attach legal value to pseudonymisation and privacy-enhancing technologies; create an operative, affirmative route to data for AI; preserve open public-sector licences; and reform supervision under a Duty to Cooperate and an Innovation Mandate. The purpose is to replace artificial scarcity, fragmentation and institutional drift with predictable, innovation-capable law.

Europe needs rules that make data usable, safeguards enforceable and public power answerable to evidence and reasons.

This article was published on 8 September 2026. At publication, Council documents ST 12535/26 and WK 13065/26 remained restricted; the analysis does not attribute unverified content to them.

First published on DigiData on 8 September 2026.