Improvements needed on the Data Acquis-related parts of the Digital Omnibus

Executive summary

On 19 November 2025, the European Commission proposed the 'Digital Omnibus,' a sweeping overhaul of EU data and AI legislation. While presented as a technical simplification, the proposal sparked strong pushback from digital rights advocates, regulators, and academics. Most attention has focused on the GDPR, ePrivacy and AI Act changes, but **equally serious shifts in data governance have received far less scrutiny.**

The proposal also merges multiple instruments into the Data Act, including the Data Governance Act and Open Data Directive, under the stated aim of boosting competitiveness and reducing legal fragmentation. The Digital Omnibus proposal rewires the EU data framework by making the Data Act the single 'hub' instrument. It repeals the Data Governance Act and the Open Data Directive, and moves their core mechanisms into new Chapters VIIa to VIIc of the Data Act. **The merger collapses distinct legal regimes with different objectives**, including data access, re-use, and governance. This creates legal ambiguity and weakens enforceability, rather than reducing fragmentation. **The risk is political: lawmakers may treat it as harmless consolidation, even as it quietly rewrites the balance of power in the data economy.** It also risks blurring the line between data governance and data protection.

Far from a routine consolidation, **the Omnibus fundamentally recalibrates who holds power over data.** The plan tilts control toward data-holding companies at the expense of public oversight and individual rights. Three main changes matter for digital rights and democratic governance: narrower public-sector access to privately held data, an expanded refusal channel for data holders in IoT access, and a lighter trust architecture for intermediation and altruism.

As with other parts of the Digital Omnibus and the wider trend toward deregulation, **lawmakers must resist any 'simplification' that comes at the expense of rights and accountability.** The proposal is presented as simplification, but it lacks a clear diagnosis of existing problems and removes or weakens safeguards without demonstrating necessity. This risks weakening people's rights and public oversight while concentrating control in data-holding companies. Moreover, the reform does not identify why existing instruments have failed to deliver uptake or what barriers prevent data sharing in practice. Evidence shows that data sharing does not primarily occur through the mechanisms promoted by the DGA, raising doubts about whether the proposed reforms address real-world practices. Without such assessment, the changes risk addressing the wrong problems and entrenching structural imbalances in the data economy.

The proposal reflects a shift from governance-focused safeguards toward facilitating data use, without sufficient safeguards or evidence that this approach serves the public interest. **EDRi does not support the Digital Omnibus.** However, if lawmakers move forward, they must address the structural flaws and remove or amend the provisions that most undermine governance and rights protection.

Key issues to be addressed

The Digital Omnibus must not be treated as technical clean-up. It rewires core parts of the EU's data system. If lawmakers proceed, the final text must preserve strong guardrails for democratic oversight, user control, and fair competition.

- **The idea of simplification cannot be used to disguise a shift in power.** The proposal rewrites key obligations and weakens protections, while claiming to streamline. The new Chapters VIIa–VIIc and Article 1 restructure the entire framework. These changes must be rejected unless they restore or improve existing safeguards, enforcement, and people's rights..
- **The revised Data Act must clearly reaffirm that it does not create new legal bases for processing personal data** (Article 1, Chapter VIIc), and that the GDPR continues to apply in full whenever personal data are involved. Clarity here is essential to avoid regulatory arbitrage and weakened rights protection.
- **Legal definitions must be clear and enforceable (Article 2)**. Vague or inconsistent concepts, such as 'trusted' data services, 'public emergency', or 'protected data,' should be tightened. Key concepts that structure the data governance framework, including 'data space', must be clearly defined in binding provisions rather than only in recitals. Rights and obligations must not depend on open-ended or politically flexible terms.
- **The revised text must resolve overlaps in scope between Chapters III and VIII and undefined legal terms.** The move into a single instrument creates the need to clearly distinguish between data access, data re-use, and governance obligations. The proposal reproduces existing inconsistencies, including the conflation of data access and data use, which risks distorting the application of legal obligations.
    - **Without explicit legal separation, the framework risks internal contradictions and inconsistent enforcement.** It also remains unclear in practice which actors fall under which regime and which set of obligations applies. This creates legal uncertainty, increases the risk of misclassification, and undermines consistent application across Member States.
    - **The merger is therefore a missed opportunity to clarify the relationship between overlapping chapters** (e.g. on public-sector re-use), eliminate divergence in the definition of public bodies, and codify key concepts such as "data space" in binding provisions. Without this, legal certainty and enforceability remain fragile.
- **The current design of business-to-government data access lacks clarity, coherence, and a clear purpose.** Limiting access to public emergencies (Article 15a) risks rendering the mechanism ineffective for public-interest uses outside crisis situations, while still leaving room for broad interpretation of what constitutes an emergency.
- **The emergency-only model** introduced in Article 15a, together with the deletion of Articles 14 and 15, **creates a framework that is both incomplete and ambiguous**. Limiting access to public emergencies risks making the mechanism ineffective in practice, while leaving room for broad and potentially discretionary interpretation. At the same time, removing non-emergency access pathways eliminates the possibility for public

authorities to act in clearly defined, high-value contexts such as health, environmental monitoring, and market surveillance.

- **The framework should instead establish a strictly safeguarded access regime** comprising both a narrowly scoped emergency pathway and a clearly defined non-emergency access mechanism based on precise legal thresholds, necessity and proportionality requirements, independent oversight, and transparency obligations. Without such a structure, and in the absence of clear institutional pathways and incentives, the mechanism risks remaining unused or being applied in an inconsistent and discretionary manner that weakens accountability, entrenches dependence on dominant data holders, and undermines people's rights.
- **Security and trade-secret concerns** (refusal ground in Articles 4(8) and 5(11)) **must not become blanket refusals**. Require data holders to offer secure-access alternatives. Refusals must be independently reviewed and fast-tracked to prevent abuse.
- **Switching exemptions in Article 31 must be time-limited and narrow.** Broad legacy-contract exceptions create long-term lock-in and undermine user choice.
- **The deletion of Article 36 removes minimum safeguards for automated data-sharing arrangements.** Where data sharing is governed by technical or automated systems, the framework must ensure enforceable baseline protections, including reliability, accessibility, and the possibility for human intervention and redress. These safeguards should not be replaced by voluntary standards.
- **The integrity of the 'trusted' data label must be protected** (Chapter VIIa). If intermediation and altruism duties are weakened, the label becomes hollow and accelerates market concentration. Rigorous obligations must stay in place. Registration must be a mandatory condition for operating data intermediation services in the Union. Only registered entities should be permitted to provide such services, and registration must trigger the full set of obligations under Chapter VIIa.
- **No hidden new legal bases for personal data.** Chapter VIIc must clearly state that it does not override or supplement the GDPR. Protected data reuse must still include secure processing, transparency, and redress.
- **Article 32's law enforcement secrecy clause must be tightly scoped**. Introduce delayed notice and reporting to prevent unchecked data access.
- **EDIB's composition under Article 41a must ensure civil society inclusion, cross-border coordination, and full transparency.** Enforcement structures must preserve the independence of competent authorities and avoid centralising functions in ways that blur responsibilities or concentrate decision-making power. Coordination mechanisms, including any centralised reporting systems, must not become substitutes for accountable and decentralised enforcement.
- **The proposal assumes that increasing data availability leads to value creation, but does not define what value is created or for whom.** Evidence shows that data sharing often occurs outside formal data market structures, raising questions about the effectiveness of the proposed model.

Top four priorities

1. No parallel regime for personal data, preserve GDPR primacy across the data framework

The Data Act must not introduce alternative pathways for processing personal data. All data-sharing mechanisms, including re-use, intermediation, and access regimes, must remain fully subject to the GDPR to prevent fragmentation, regulatory arbitrage, and weakening of people's rights.

2. Ensure that data access frameworks are usable, accountable, and do not reinforce dependency (Articles 14, 15, 15a; Articles 4(8), 5(11))

Data access rules must not be designed in ways that render them ineffective in practice or allow dominant data holders to control access. This requires restoring a workable business-to-government access framework beyond emergencies and strictly limiting refusal grounds, with independent review and enforceable safeguards. Otherwise, public authorities and third parties remain dependent on voluntary access controlled by large actors.

3. Prevent concentration of power in data governance and enforcement structures (Chapter VIIa; Article 41a; reporting mechanisms)

The framework must not create a nominal 'trust architecture' or centralised coordination mechanisms that concentrate power without accountability. Data intermediation must be subject to mandatory registration and enforceable obligations, while enforcement structures must preserve the independence of competent authorities and avoid centralisation that enables indirect influence or uneven application.

4. Guarantee that rights and obligations are clear, enforceable, and usable in practice across the framework

The merger of regimes must not result in legal ambiguity or operational uncertainty. Actors must be able to determine which rules apply, and authorities must be able to enforce them consistently. This requires clear legal definitions, explicit separation of regimes (access, re-use, governance), and mechanisms that are not only well designed on paper but also supported by institutional pathways and incentives for effective use.

What changes in the Digital Omnibus

The proposal explicitly frames its "data acquis" part as consolidation: **it integrates Data Governance Act mechanisms and Open Data Directive reuse rules into the Data Act, and repeals the former instruments.**

Primary legal moves that affect the Data Act and related instruments are:

- The Digital Omnibus amends Regulation (EU) 2023/2854, adding new subject-matter items (voluntary registration of intermediation and altruism, EDIB, data localisation, and re-use of public-sector and research data).
- It expands the Data Act trade-secret refusal mechanism in IoT data access to cover 'high risk' of unlawful access or disclosure to third-country-controlled entities, not only 'serious economic damage.'
- It narrows business-to-government requests to a public-emergency basis in a new Article 15a, and adjusts the procedural regime around it.
- It adds transitional exceptions in cloud switching for significantly customised services and for SMEs and small mid-caps, including possible early termination penalties.
- It deletes the Data Act's smart-contract minimum requirements provision (Article 36).
- It broadens the Data Act's protection against unlawful third-country governmental access to non-personal data, extending the duty to new actors involved in re-use, intermediation, and altruism, with a notice exception for law enforcement-type requests.
- It inserts new Chapters VIIa (intermediation and altruism), VIIb (data localisation and data availability to competent authorities, plus cross-border access safeguards), and VIIc (re-use of certain data and documents held by public sector bodies and public undertakings, plus research data).
- It repeals the Data Governance Act, the Free Flow of Non-Personal Data Regulation, and the Open Data Directive, with a correlation-table approach.
- The consolidation process leaves unresolved overlaps in scope and terminology across the original instruments. It does not clarify whether definitions from public procurement law apply, or how chapters with overlapping subject matter interact. These gaps create interpretive risks that undermine legal certainty and operational consistency. These issues stem from the merger of instruments with different legal logics, which should not be combined without clear conceptual separation.
- It also misses the opportunity to align sectoral and horizontal data law terminology. Terms like 'data holder' and 'health data holder' diverge across instruments, while key concepts like 'data space' are left undefined. These gaps matter operationally and legally, especially as more rules depend on fine-grained categorisation of actors and datasets.

In sum, **the Omnibus tilts control over data toward the companies that hold it, moving away from treating data as a public-interest resource governed by strict rules.** This shift occurs without demonstrating that existing safeguards are ineffective or that the proposed changes address identified failures. In addition, **repealing three separate instruments risks leaving gaps if the transferred provisions are weakened, narrowed, or stripped of enforcement structure.** What appears as streamlining can in practice mean losing safeguards without replacing them.

Granular analysis

Trade secrets and third-country leakage refusal ground in IoT data access

The Digital Omnibus replaces Data Act Article 4(8) and Article 5(11). It keeps the 'serious economic damage' basis and adds a second refusal basis: 'high risk' of unlawful acquisition, use, or disclosure to third-country entities or EU entities under their control, in jurisdictions with weaker protection.

The Data Act IoT access rules can be viewed as 'users can get and share their device data.' The Omnibus expands the situations where a manufacturer or service provider can say no, using trade-secrets and third-country risk arguments.

Risks

- **This is not only about business secrets.** IoT product data can be personal, mixed, or inferential. When refusals rise, users lose practical control and third-party access collapses, which weakens autonomy and can indirectly hinder rights like repair choice, switching, and consumer empowerment. This also affects people's ability to exercise control over data generated by devices they use.
- **Competition and accountability:** this refusal channel sits exactly where aftermarket markets form (repair, insurance, energy optimisation, mobility services). Data holders can become de facto gatekeepers of data generated by products. More refusal discretion increases that risk.
- **Private concentration risk:** data holders can operationalise 'foreign risk' as a default argument to block data access to smaller competitors who rely on overseas tooling, ownership, or investment structures, even when no realistic trade-secret harm exists. "High risk" can become a low-evidence claim if enforcement capacity is weak, especially for SMEs challenging refusals.
- **State overreach risk:** where private actors can block user-driven access, governments may push for alternative mandatory access channels that can be less rights-protective, because the user-centric channel stops working.

Recommendations

- Protecting trade secrets and guarding against unlawful third-country access are legitimate goals. But they **must not be used to deny users, competitors, or watchdogs legitimate access to data**. The law must require secure-access alternatives and fast, independent review of any refusal.
- **Any refusal based on third-country risk must be last resort.** The data holder must first offer a workable secure-access alternative that enables legitimate use without disclosing secrets.
- **Refusal decisions must be reviewable** fast by an independent authority, with transparency towards the requesting user or recipient and effective redress.

Business-to-government access narrowed to public emergencies

The Omnibus replaces the Chapter V title and deletes Data Act Articles 14 and 15, inserting a new Article 15a that limits requests to public emergency response and recovery. It constrains the requested data to non-personal data where possible, and allows personal data only where non-personal data is insufficient, ideally in pseudonymised form.

Under the current Data Act, public bodies can request certain private-sector data in 'exceptional need' cases. The Omnibus removes these pathways and narrows access to public emergencies and closely related needs. This results in a framework that is both structurally incomplete and legally ambiguous, combining a narrow trigger with broad interpretative uncertainty.

Risks

- **Ambiguity of the emergency trigger:** While a narrower trigger may reduce mission creep, the concept of 'public emergency' remains open to broad and potentially discretionary interpretation. A narrow label alone does not function as a safeguard. Without clear legal criteria, independent validation, and transparency, the risk of over-expansion remains.
- **Structural governance gap:** Removing Articles 14 and 15 eliminates non-emergency access pathways and limits the ability of public authorities to act in clearly defined, high-value contexts such as AI-driven health systems, environmental monitoring, and market surveillance. This weakens evidence-based policymaking and creates a structural accountability gap.
- **Private concentration and dependency:** In the absence of non-emergency access mechanisms, dominant data holders can effectively control access to data outside crisis situations. Public authorities become increasingly dependent on voluntary data sharing or procurement, often under conditions that favour large providers, reduce transparency, and increase costs, particularly for smaller administrations.
- **Inconsistent and discretionary application:** A system limited to emergencies risks becoming either unused in practice or applied in an ad hoc manner. Without clear thresholds and governance structures, access decisions may vary across Member States and contexts, undermining legal certainty and equal treatment.
- **Institutional feasibility risks:** Even where safeguards are well designed, the absence of clear institutional pathways, governance structures, and incentives for public authorities to use such mechanisms may limit their practical use. This risks leaving the framework formally in place but operationally irrelevant.
- **State overreach risk:** The use of 'public emergency' as a legal trigger can enable broad access if not strictly constrained. Personal data access in crisis contexts may expand rapidly unless strict minimisation, purpose limitation, and deletion obligations are clearly defined and enforced.

Recommendations

- Replace the current emergency-only model with a coherent and strictly safeguarded access regime comprising both:
  - a narrowly scoped emergency pathway (Article 15a), and
  - a clearly defined non-emergency access mechanism replacing Articles 14 and 15.
- Any non-emergency access mechanism must be based on precise legal thresholds and conditions, avoiding ambiguous concepts such as 'exceptional need', and must be subject to strict necessity and proportionality requirements, independent oversight, and transparency obligations.
- Emergency access must be strictly defined and constrained. It must not become a backdoor for routine access or a discretionary tool for broad data collection.
- Ensure that both emergency and non-emergency mechanisms include clear procedural frameworks, accountability structures, and incentives for use, to avoid underutilisation and ensure consistent application across Member States.
- Personal data must remain exceptional. Use anonymised data by default and allow pseudonymised personal data only where strictly necessary, with DPA involvement, oversight, and enforceable safeguards.

Cloud switching exemptions that prolong lock-in

The Omnibus inserts new paragraphs in Data Act Article 31. It exempts significantly customised services under legacy contracts from most Chapter VI obligations (except parts of Article 29), allows proportionate early termination penalties in fixed-duration contracts for certain service types, and extends relief to SME and small mid-cap providers for legacy contracts.

The Data Act aims to enable effective switching between cloud providers and reduce lock-in. The Omnibus introduces broad exemptions for legacy contracts and 'customised' services, allowing switching restrictions and penalties to persist across a significant share of the market.

Risks

- Lock-in and reduced resilience: Switching rules are not only a competition issue. They directly affect the ability of users to change providers in response to security risks, pricing changes, or geopolitical dependencies. Broad exemptions allow contractual lock-in to persist, limiting flexibility and resilience.
- Structural advantage for incumbents: The breadth of exemptions favours large providers, who can standardise 'customisation' as part of their service offerings. Smaller providers and customers face greater legal and negotiation burdens, reinforcing asymmetries in the market.
- Circumvention of switching obligations: Providers may design service tiers in ways that qualify as 'customised' in order to fall outside the effective scope of switching rules. This

risks turning exceptions into the default and undermining the core objective of the Data Act.

- Entrenchment of dependency: Prolonged lock-in increases reliance on dominant cloud providers, particularly for SMEs and public bodies that lack the capacity to renegotiate contracts or absorb switching costs. This creates long-term dependency risks and weakens bargaining power.

Recommendations

- Reject broad carve-outs that allow switching restrictions and penalties to persist under the guise of legacy contracts or customisation.
- Any exemption for customised services must be narrowly defined and limited to genuinely bespoke arrangements, with clear criteria to prevent circumvention.
- Legacy-contract exemptions must be strictly time-limited and must preserve effective switching and portability rights in practice.
- The framework must ensure that switching obligations remain enforceable across the market and are not undermined by contractual design or categorisation practices.

Third-country governmental access and data localisation governance

The Omnibus replaces Data Act Article 32(1) and (2), extending the duty to prevent unlawful third-country access to non-personal data beyond cloud providers to actors involved in public-sector re-use, re-users, intermediation services, and altruism. It also includes a notification duty to affected persons, with an exception where the request serves law enforcement purposes.

The law tells certain actors holding non-personal data in the EU to resist unlawful third-country government access requests, and to notify affected parties, except when secrecy is claimed for law enforcement reasons.

Risks

- Sovereignty and rights: strengthening this protection is positive, especially as more protected public-sector data and re-use mechanisms expand. If the EU encourages data availability, it must also reduce exposure to compelled access from outside the EU.
- Accountability gap: a wide 'law enforcement purpose' notice exception creates a weak point. It may become the default label for secrecy. The law-enforcement notice exception can normalise non-notification, undercutting affected parties' ability to challenge access.
- Private concentration risk: larger providers can absorb compliance and legal assessment costs, while smaller intermediaries struggle, leading to consolidation pressures.
- Data localisation policies can improve security but also risk fragmentation if not narrowly scoped. Any localisation requirements must be justified, proportionate, and not used to

entrench dominant infrastructure providers.

Recommendations

- Support extending protections against unlawful third-country access to all actors newly drawn into the re-use and intermediation framework.
- Any law enforcement secrecy exception must be narrow, documented, and paired with delayed notification and transparency reporting. Amendments should push for delayed notice rather than silent notice, with strict conditions and transparency reporting.

Smart contracts safeguards removed

The Omnibus deletes Data Act Article 36. The proposal removes binding minimum requirements for smart contracts used to execute data sharing agreements.

Risks

- Accountability and security: deleting the legal baseline shifts risk into private contracting and voluntary standards. That disadvantages SMEs and public bodies that cannot negotiate technical safeguards on equal terms.
- Private concentration risk: larger providers can impose contract terms and proprietary implementations, and smaller counterparties accept them.
- State overreach risk: if public procurement relies on smart-contract governed sharing without minimum safeguards, public bodies may deploy weaker systems with downstream rights impacts. This is a governance risk.

Recommendations

- Reject deleting smart-contract safeguards without replacing them with enforceable minimum requirements.

Trust architecture: data intermediation services and data altruism moved and softened

The Omnibus adds Chapter VIIa on data intermediation services and data altruism organisations, with public Union registers and a 'recognised' label.

The DGA's 'trusted intermediary' and 'data altruism' model moves into the Data Act. The package educes obligations and shifts toward a voluntary model for these mechanisms. Any entity providing data intermediation services within the meaning of this Chapter must fall within this

mandatory registration requirement, to prevent avoidance through reclassification or functional design.

Risks

- Trust and oversight: the core risk is the 'trust gap.' If the EU keeps the label but weakens enforceable obligations, users and smaller organisations may rely on the label and share data under false confidence. The EDPB and EDPS stress the importance of trustworthy and responsible data sharing and recommend maintaining safeguards favouring transparency and oversight. Empirical evidence shows that the value of intermediation services lies in their ability to demonstrate trust and neutrality. Weakening obligations undermines this core function.
- GDPR coherence: altruism and intermediation can touch personal data directly. Any 'altruism' framing must not create parallel regimes that are easier to misuse than GDPR pathways.
- Private concentration risk: functional separation is harder to audit than legal separation. Dominant platforms can internalise 'intermediary' roles while preserving conflicts of interest. 'Recognised' services can become market-favouring badges, driving consolidation.
- State overreach risk: if oversight weakens, public bodies may route data-sharing via intermediaries with insufficient safeguards, creating indirect access channels with weaker accountability.

Recommendations

- Reject the weakening of obligations for data intermediation and data altruism services.
- Data intermediation services must be subject to mandatory registration as a condition for operating within the Union. Only registered entities should be permitted to provide such services, and registration should trigger the application of all obligations under this Chapter.
- Recognised intermediation must require strong separation and a strict ban on using shared data for the intermediary's own purposes, including advertising and profiling.

Re-use of protected public-sector data, public undertaking data and research data

The Omnibus inserts Chapter VIIc establishing rules for re-use and practical arrangements, including protected data held by public sector bodies and certain public undertakings and research data. The merger combines regimes with different objectives and safeguards, which risks weakening the protections originally designed for protected data. At the same time, it remains unclear in practice which actors fall under which regime and which set of obligations

applies. This lack of clarity undermines legal certainty, creates enforcement challenges, and increases the risk of inconsistent or selective application. This ambiguity may allow actors to structure their activities to fall within less stringent regimes, further undermining the effectiveness of the framework..

It also allows higher fees and special conditions for very large enterprises, including gatekeepers under Regulation (EU) 2022/1925, and introduces competent bodies and redress structure.

The EU merges two regimes that used to be separate: open data re-use rules, and the DGA system for allowing re-use of non-open protected data under strict conditions. The goal is one coherent re-use framework inside the Data Act.

Risks

- Privacy and GDPR coherence: the re-use framework should not itself create an obligation to allow re-use of personal data and does not provide a legal basis for access.
- Governance: merging regimes can reduce fragmentation, but only if the protected data safeguards remain. The DGA was explicitly built around trust conditions for protected data re-use and for neutrality in data sharing.
- Competition and public interest: the gatekeeper-related fee and condition logic can be pro-competition if carefully constrained. If it becomes an ad hoc discriminatory pricing tool, it can backfire and reduce transparency.
- Private concentration risk: without strict safeguards, protected data re-use can feed data brokerage and downstream re-identification. Higher-fee discretion without harmonised criteria can create unequal access patterns and legal uncertainty.

Recommendations

- Anyconsolidation must preserve the DGA's protected-data safeguards and makes GDPR precedence explicit for mixed datasets.
- The framework must address risks associated with non-personal data, including re-identification, aggregation harms, and exposure to third-country access.
- The re-use framework must never be read as creating a new legal basis for personal data processing or a duty to disclose personal data.
- Any gatekeeper or 'very large enterprise' fee regime must be transparent, non-arbitrary, and reviewable.

Enforcement and governance: EDIB, complaints, and the repeal of core instruments

The Omnibus inserts a new Article 41a establishing the European Data Innovation Board, and replaces Article 42 defining EDIB's role.

It also updates the complaint mechanism (Article 38) and includes a carve-out from the sanctions article for Chapter VIIc.

Finally, it repeals the DGA, the Free Flow of Non-Personal Data Regulation and the Open Data Directive.

The proposal changes who coordinates and how enforcement cooperation works. It also removes the separate legal acts that used to carry governance structures, and moves them into the Data Act.

Risks

- Coordination risk: unclear allocation of responsibility between regulators can create accountability gaps and delays.
- Accountability risk: if it's unclear which authority is responsible, enforcement will fall through the cracks. Strong cooperation and clearly assigned roles are critical to avoid loopholes.
- Legitimacy risk: turning the EDIB into a closed forum of authorities could sideline civil society and independent experts. Transparency and stakeholder inclusion are needed so that decisions aren't made in a vacuum.
- Private concentration risk: if enforcement coordination weakens or is patchy, dominant companies can exploit the gaps, playing regulators off each other or evading effective oversight.
- Redress risk: fragmented oversight and redress mechanisms (especially for the new data re-use chapter) could leave individuals and smaller organisations without an effective way to challenge abuses or mistakes.

Recommendations

- A single instrument can only function if enforcement roles are clear and cooperation with DPAs is mandatory where personal data is involved. Enforcement roles must be explicitly defined, and cooperation frameworks must ensure effective oversight across jurisdictions.
- EDIB must operate transparently and should include structured participation from civil society, academia, and consumer organisations.
- The final text must explicitly prevent enforcement asymmetries. Large actors should not be able to game differing national practices or delay remedies through fragmented governance structures.
- The broader Digital Omnibus also introduces proposals for centralised incident reporting portals. These should remain outside the Data Act, and any future implementation must respect data minimisation, national oversight, and clear legal limits on how such data are accessed or reused.
- Centralised reporting mechanisms risk concentrating operational and informational power in ways that can undermine the independence of competent authorities. They may blur responsibilities, create asymmetries in access to information, and enable indirect

influence over national regulators. Any coordination mechanism must therefore include strict safeguards to preserve institutional independence, ensure clear allocation of responsibilities, and prevent centralisation from becoming a substitute for accountable and decentralised enforcement.