Closing the EU Enforcement Gap

Three steps to make digital rules count in practice

Strategy Notes
By Kai Zenner and Maria Koomen, 1 September 2026

The EU has spent fifteen years building the world's most dense digital regulatory framework, yet without sustained, independent enforcement, the digital laws it has created cannot deliver what they have promised. This goes back to a structural problem: Enforcement is fragmented across various regulatory bodies, chronically under-resourced, and vulnerable to political interference and pressure by stakeholders at precisely the moments when independence matters most. The gap between the laws on paper and actual compliance is widening.

Several root causes underlie the dysfunction: geopolitical exposure invites external interference; accountability dissolves when enforcement meets politics; governance fragments across too many bodies; capacity is stunted by chronic resource shortfalls; and national interests persistently dominate European interests in digital enforcement.

This paper proposes a three-step reform path to address root causes and close the enforcement gap:

1. In the short term, the EU should establish a **Digital Regulation Cooperation Forum** (EU DRCF), modelled on the UK's successful equivalent, and built on existing European Data Protection Supervisor (EDPS) infrastructure.
2. In the medium term, coinciding with the 2028–2034 Multiannual Financial Framework (MFF), the EU should transform the existing European Health and Digital Executive Agency (HaDEA) into a **Digital Enforcement Agency** (DEA) with independent powers to investigate, audit, and enforce EU law against the largest digital platforms, GPAI model providers and other designated actors.
3. In the long term, the EU should adopt treaty-level reforms to enable fully **independent enforcement agencies across the entire Digital Single Market** – covering not only platforms, data, and AI but also cybersecurity, connectivity, and competition.

The EU has an enforcement gap

171 digital laws, 315 regulatory bodies, and a European Commission that simultaneously legislates, enforces, and evaluates while negotiating deals with foreign powers. The problem comes down to a structural inability to uphold the rules.

Transforming an existing agency is faster, cheaper, and more durable

HaDEA provides the institutional foundation; the Commission's enforcement teams provide the expertise; the MFF cycle provides the political vehicle. No new EU agency, no standalone legislative proposal, no treaty change debate.

Coordination alone will not close the gap

Existing proposals are either legally sound but institutionally weak, or constitutionally fragile without treaty change. A sequenced reform approach – EU DRCF first, then a DEA – tackles this political hurdle by building on existing institutions rather than creating new ones.

Legal certainty is a strategic asset

A European Commission with enforcement susceptible to interference and endless appeals is ultimately both a weak enforcer as well as a weak geopolitical actor. Structural delegations remove exploitable leverage and turn digital law from a negotiating chip into a credible commitment for European markets and societies.

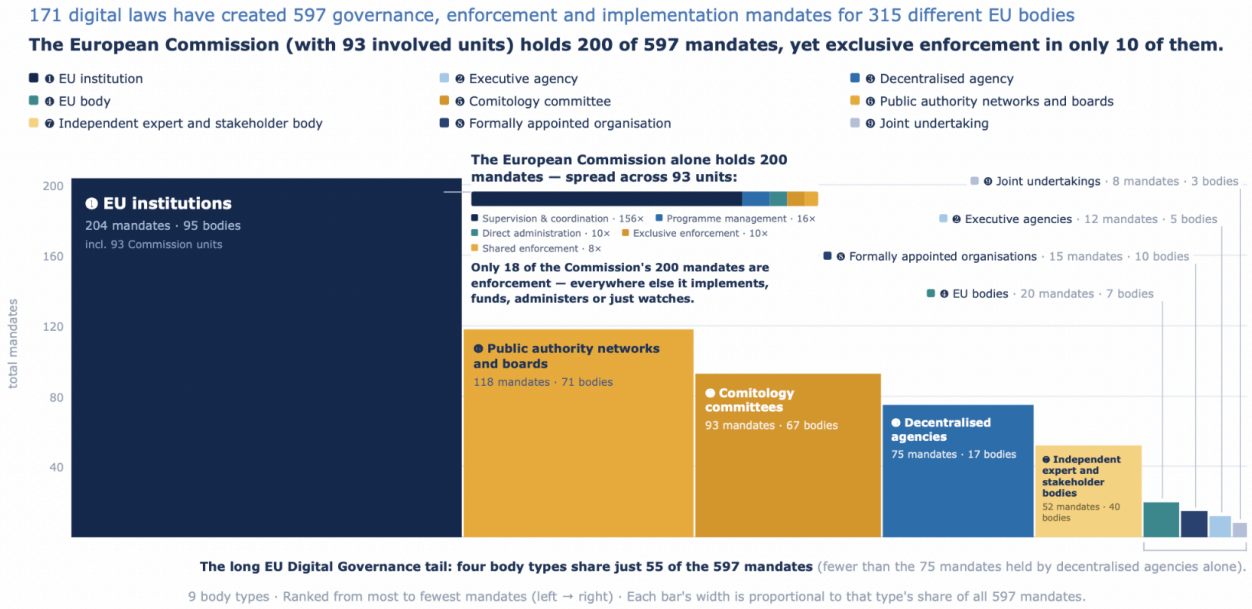
The state of EU digital law enforcement

Over fifteen years, the EU has made itself the world's standard-setter for technology governance, building an unusually dense architecture of digital laws[1] – GDPR, the Copyright Directive (CDSM), DMA, DSA, AI Act, Data Act, and NIS2 chief among them.

Creating laws is one thing; enforcing them is another. More and more research findings point to a structural enforcement gap,[2] resting on two observations:

First, enforcement is highly fragmented. Responsibility is dispersed across hundreds of overlapping EU and national mechanisms. Mario Draghi counted 270 regulators that are active in digital networks across the Union, including all 27 Member States.[3] At the EU level alone, according to our own research, 315 different bodies carry 597 mandates for governance, enforcement, and implementation. The European Commission carries a third of the overall mandates – of which only 18 are enforcement mandates (10 exclusive, 8 shared with member states), and they cover just 12 of the 171 digital laws. The resulting oversight architecture looks different from one law to the next, from one member state to another, and at each level. This patchwork has grown not only by creating new regulators for most new laws, but also by repurposing existing regulators: some national data protection authorities (DPAs) created for the GDPR, now double as market surveillance authorities for the AI Act, while others do not, compounding the confusion.

Figure 1: The EU's digital governance long tail



Source: Based on research done by Kai Zenner and J. Scott Marcus for a forthcoming CEPS publication.

Second, compliance is weak. The behavioural changes tech companies have made (e.g. Apple opened its app store, Google restructured search, Meta offered consent alternatives) were designed to satisfy the letter of the law while preserving the overall commercial logic as well as market structures that these rules were meant to disrupt. One could say that “partial compliance” has become the norm. Where enforcement did arrive, it confirmed the gap rather than closing it: noyb’s Max Schrems documents that 99.93% of complaints to Ireland’s Data Protection Commission are dismissed without a substantive decision and the Irish DPC has never completed a single inquiry into Google.[4] [5] Application is also strikingly uneven: in 2024 the German, Spanish, and Italian DPAs issued 416, 281, and 140 fines respectively, while a dozen member states issued fewer than ten.[6]

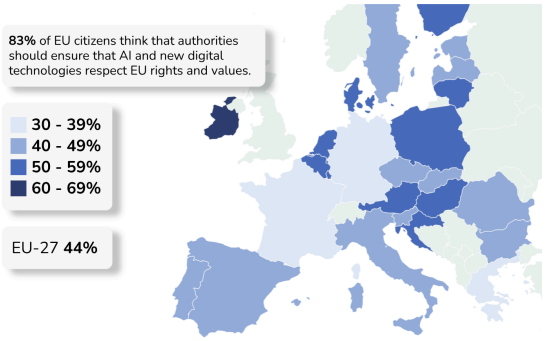
Centralisation and simplification were presented as solutions. Recognising the failures of decentralised enforcement, the EU vested the European Commission with primary authority under

the DMA, the DSA, and – for GPAI models – the AI Act. Yet centralisation alone proves insufficient, as enforcement remains inconsistent and exposed to political interference.

Independence is a decisive ingredient, though not sufficient on its own. The September 2024 ECJ rulings – upholding a €13 billion Apple state-aid recovery and a €2.4 billion Google antitrust fine – showed that enforcement can prevail against aggressive litigators when independent courts shield it from that pressure. Yet even these penalties leave their targets' business models intact: Google reportedly cleared its €2.4 billion fine in just fourteen days of business, and the €120 million DSA fine against X is, on its own, too small to alter the conduct of a company backed by a trillionaire.[7] For platforms of this power and scale, an isolated fine is merely a cost of doing business; what could change conduct is sustained, predictable enforcement, not just one-off penalties.

Figure 2: Only 44% of EU Citizens feel well-protected in the digital world

Share of respondents who think that the EU protects their rights in the digital world (very) well



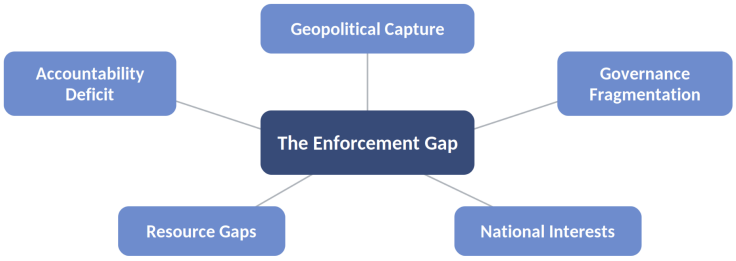
26,319 EU citizens surveyed Feb.-Mar. 2025
Sources: Statista, European Commission, Eurobarometer

Simplification has done no better. The 2024 Draghi[3] and Letta[8] reports diagnosed regulatory fragmentation and under-enforcement, but Brussels read them selectively as symptoms of EU overregulation, culminating in the November 2025 Digital Omnibus. The systemic causes behind increasing compliance costs for SMEs or duplicated cyberattack notification procedures, however, remain untouched: chaotic deregulation has merely superseded chaotic regulation.[9] The blindspot in both centralisation and simplification efforts is the same: enforcement itself.

The enforcement gap: Why EU digital laws fail in practice

If problems persist despite a decade of counter-measures, the root causes deserve naming (see Figure 3). To start, the European Commission has become increasingly powerful. The institution has shifted from impartial treaty guardian to an exposed geopolitical actor: a trajectory institutionalised under Juncker and reaching its apex with von der Leyen's avowedly "geopolitical Commission."[10]

Figure 3: Root causes of enforcement gap



An EU institution that simultaneously sets the political agenda, legislates, enforces, and evaluates its own laws produces five distinct enforcement challenges.

Geopolitical exposure invites external interference: As the Commission takes on enforcement under the DSA, DMA, and AI Act, it is also negotiating global trade and security. Yet, regulatory credibility depends on independence. In 2025, after US tariff threats, it delayed its DMA decisions against Apple and Meta, dragging the DMA "into the global trade war."[11] [12] In early 2026, in what over thirty civil society organisations called a capitulation to US pressure, President von der Leyen personally directed the delay of a Google Search fine that DG COMP had already prepared.[13] The exposure is structural: Europe depends on US tech firms for its own digital infrastructure, and on US security guarantees in conflicts on its external borders. More insidiously still, the Commission may under-enforce pre-emptively, to avoid pressure on its foreign-policy hand.

Accountability dissolves where enforcement meets politics: Acting as a "deal maker"[14] with member states, the Commission has incentives to spare national champions when their governments' support is needed for legislation or the EU budget. Companies learn from these political signals and treat compliance as negotiable: digital-industry lobbying in Brussels rose from €97 million in 2021 to a record €151 million in 2025, with the five largest US platforms logging more than one Commission meeting per day.[15] Such "enforcement bias" corrodes the digital rulebook's credibility and distorts competition, defeating the very competitiveness agenda it is meant to serve.[16]

Governance is fragmented and over-complex: Applicable digital laws have grown from roughly 20 in 2010 to 171 today;[1] a single service such as TikTok's recommender system must satisfy DSA, GDPR, AVMSD, and AI Act obligations at once, each under a different oversight architecture and timeline.[17] With 315 bodies involved in implementing and enforcing the digital rulebook at the EU level alone, execution and coordination are widely judged inadequate.[1] This fragmentation creates duplication, delay, and the forum shopping that a single, well-resourced EU regulator could remove, sparing claimants today's task of navigating multiple authorities to vindicate one right.

Regulator resources and capabilities fall short – and are exploited: National authorities vary dramatically. Ireland's DPC – lead regulator for most US platforms – is criticised as under-resourced and under-enforcing[4] [18], while France, Italy, and the Netherlands act far more assertively. Italy's 2023 emergency order against ChatGPT is probably the best-known case.[19] Most member states lack the expertise to supervise AI Act or NIS2 obligations. Well-resourced tech firms compound this by exploiting the appeals architecture systematically: the Google Shopping case ran more than seven years from the infringement decision to the final dismissal of Google's appeal, with the conduct continuing throughout. Capacity shortfalls also open a subtler channel for capture: reliance on external experts with undisclosed ties to the companies under scrutiny.[61] Where regulators lack in-house technical capacity, dependence on outside expertise is often unavoidable – but without disclosure requirements and enforceable limits, it becomes another channel through which regulated companies shape the rules meant to bind them.[62]

National interests erode uniform application: The EU makes independence a legal obligation when it delegates to national authorities, for example in the GDPR, yet member states remain tempted to shield domestic industries or avoid politically costly action.[20] When even the Commission hesitates to open infringement proceedings against member states for fear of upsetting Council dynamics[21], the uniform application of EU law is sacrificed to expediency. Ironically, at the supranational level – where the Commission combines legislative, political, and enforcement functions – no equivalent independence requirement applies at all.

Existing proposals to reform EU tech governance

The status quo's unsustainability is widely recognised in Brussels and several reform proposals have emerged. They range from internal coordination to fully independent enforcement.

At the lighter end sit coordination mechanisms. Ryan et al. proposed a whole-of-Commission approach[22] that would create an internal Digital Enforcement and Resilience Taskforce of senior officials drawn from the relevant DGs, using existing instruments and requiring no new legislation. A group of Commission officials proposes a three-layered structure[23] – national Digital Ministries, a Digital Coordination Unit in the Secretariat-General, and a Digital Policy Board for member states bridging the two. The EDPS's Digital Clearinghouse 2.0[24] would establish a permanent multi-stakeholder forum operating on "variable geometry," with a secretariat modelled on the UK's DRCF and a narrow legislative base for information-sharing. The 2019 German Digital Markets Transformation Agency[25] would gather and analyse market intelligence – explicitly without enforcement powers – on the model of the European Environment Agency.

At the heavier end sit independent authorities. The Robert Schuman Foundation's independent EU competition authority[26] – echoed by senior MEPs[55, 59] – would split investigation from decision-making, leaving DG COMP to investigate while a separate body decides, for instance, phase-two mergers. CERRE's European Digital Agency[28] goes furthest, potentially absorbing the Commission's DSA, DMA, and GPAI enforcement powers and pairing an EU-level regulator with consolidated national ones – an arrangement modelled on banking's Single Supervisory Mechanism. DSA-specific variants of such an independent agency have been advanced by Mariniello and Jaursch as well as political groups such as Renew Europe and the Greens/EFA.[16, 29, 30, 31]

Each proposal targets a real defect, but none addresses all five root causes (see Figure 3) at once: the coordination models remain legally sound yet institutionally weak, while the independent authority models are constitutionally fragile without EU treaty change.

Figure 4: Comparing existing reform proposals

Proposal	Originator	Independent enforcement power?	Legislative change required?	Treaty change required?
Whole-of-Commission approach	Ryan et al.	No: Coordinates existing enforcement functions only.	No: Uses existing instruments.	No
Three-layered digital governance structure	Commission officials	No: Coordination and information-sharing only.	Yes: Member states obliged to create national digital ministries.	No
Digital Clearinghouse 2.0	European Data Protection Supervisor	No: Issues joint guidance and coordination protocols only.	Yes: Targeted legislative intervention to establish legal basis for cross-authority information sharing	No
Digital Markets Transformation Agency	German Commission "Competition Law 4.0"	No: Collects and analyses market and technical information only.	No: The Commission can itself establish a new executive agency.[1a]	No
Independent EU Competition Authority	Robert Schuman Foundation	Yes: Phase two merger decision-making transferred from Commission to independent competition authority; DG COMP retains investigative role.	Yes: Primary legislation to separate investigative and decision-making functions.	Yes
European Digital Agency	CERRE[2a]; authors of DSA-specific variants	Yes: Could take over Commission enforcement powers for DSA, DMA, and GPAI models (AI Act).	Yes: Requires delegation of Commission enforcement powers, creation of new agency, and national regulator restructuring.	Not necessarily

Legal and political hurdles: Why these proposals have not succeeded

Four key obstacles – legal doctrine, institutional self-interest, fiscal constraint, and political contestation – narrow the feasible reform options in Brussels far more than each of the six presented proposals alone would suggest (see Figure 5).

Since the Court of Justice's 1958 Meroni ruling, EU agencies may exercise only clearly defined executive powers and must be kept from wide discretion that amounts to policy-making. The 2014

[1a] Legal base for the Commission to create executive agencies in Council Regulation (EC) No 58/2003.

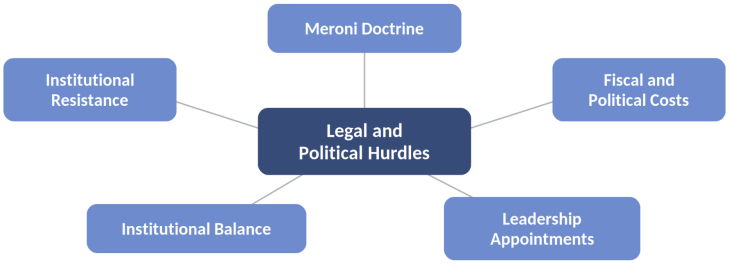
[2a] CERRE's membership includes several of the companies that would fall under such an agency's jurisdiction.

ESMA judgment softened this – permitting delegated discretionary powers where they are precisely framed and bounded[27] [32] – but the fine line between execution and autonomous judgment still matters. This produces the central dilemma of every enforcement reform: coordination mechanisms are legally safe but institutionally weak – as Mariniello notes, the Commission cannot be both a politically led executive and a credible regulatory watchdog[33] – whereas genuinely independent authorities remain constitutionally fragile without EU treaty change.

New arrangements must preserve both the Commission's prerogatives and member state implementation roles. Proposals to concentrate enforcement in standalone regulators have drawn resistance from national capitals – for instance, Ireland guarding its role as host to most of the US platforms[35] and Germany defending federal and state competences[29] – even as smaller member states concede they cannot enforce 171 laws alone and the Council of the EU calls for stronger EU-level governance.[37] The Commission welcomes centralisation when it is the beneficiary (i.e. DMA, DSA, AI Act) but at the same time resists transferring powers to independent bodies. Commission insiders often stress the synergies of keeping implementation and enforcement under one roof, yet in reality that proximity does not produce coherence. The AI Office and the DMA / DSA teams have struggled to coordinate on shared problems such as deepfakes.

Germany's 2019 Commission "Competition Law 4.0" proposal tried to sidestep the resistance by limiting its agency to information-gathering – which is precisely why it would prove insufficient, since the crisis stems from an inability to act, not an absence of information.

Figure 5: Obstacles to enforcement reform



Member states are also reluctant to fund EU reforms whose costs come now and benefits later. New EU bodies require significant investment, which is tricky when maintaining existing ones already proves difficult. The Commission, for example, faces a 76% staffing shortfall for DMA supervision alone.[38] A decade of crises, excessive deficit proceedings against eight member states in 2024,[39] and a more eurosceptic Parliament as well as public opinion raise the political price of any reform proposal that expands Brussels' budget or reach.

Whenever new EU bodies are discussed, the spectre of politicised appointments arises. Episodes from Selmayrgate[40] to the contested nomination of the EPPO's chief prosecutor,[41] the Commission's alleged attempt to install one of its own as European Data Protection Supervisor[42], and Ireland's appointment of a former Meta lobbyist as Data Protection Commissioner[43] show how difficult full independence is to secure when so many powerful interests are in play.

A sequenced three-step approach to closing the enforcement gap

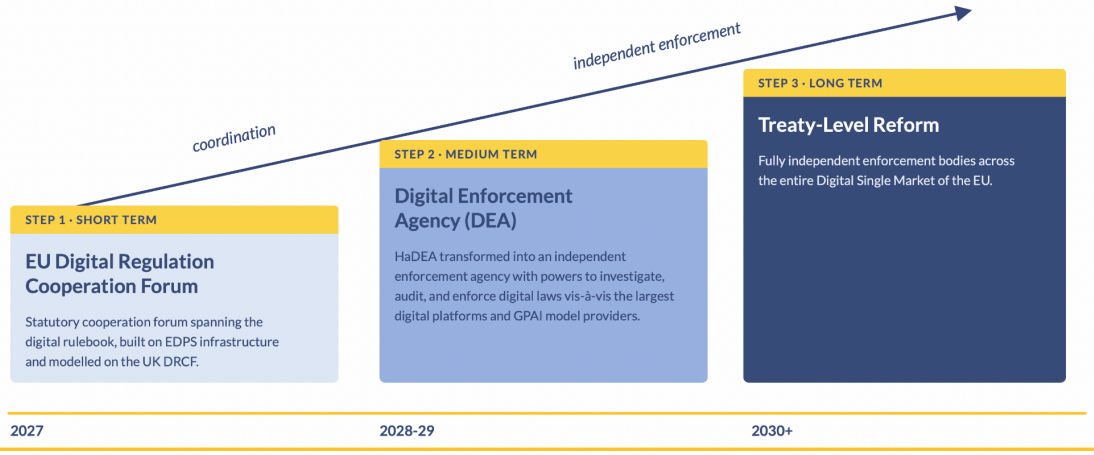
Closing the enforcement gap requires balance: building enforcement effective enough to overcome the structural problems (see Figure 3), yet bounded enough to respect the Meroni Doctrine and institutional balance, and to avoid political resistance, not least over leadership appointments (see Figure 5), that has so far undermined the build-up of comparable bodies.

None of the presented reform proposals (see Figure 4) manages to strike that balance. Pure information coordination stays safely within legal and political limits, but it is too weak to close the enforcement gap. Establishing wholly new public authorities on EU level would be powerful enough to enforce, but has proven too contested – legally and politically – to establish. However, this impasse can be overcome by sequencing rather than choosing. Such a phased approach builds enforcement capacity gradually, earning the legal and political acceptability that a single leap

cannot, by combining immediate digital governance improvements with longer-term structural enforcement reform in the digital sector.

We propose that the EU Institutions agree to execute the following three steps:

Figure 6: A phased reform approach



Step One: Establish an EU DRCF for a more coherent digital governance

In the short term, the creation of a horizontal coordination mechanism – building on the DMA High-Level Group and mirroring the UK's Digital Regulation Cooperation Forum (DRCF) – offers a legally-sound, politically-feasible, and budget-friendly starting point. By enhancing institutional trust, developing shared methodologies, and demonstrating the value of cross-regulatory cooperation, an EU DRCF would lay the political and technical groundwork that Step Two requires. Our blueprint for creating the EU DRCF is as follows:

Legal base: The EU DRCF should be established as a formal advisory body through a targeted Digital Governance Omnibus[3a], amending the relevant digital laws rather than introducing a new standalone regulation, while modelled structurally on the GDPR's establishment of the EDPB. In doing so, this approach would fulfil the ambition of the EDPS's Digital Clearinghouse 2.0 – which held its inaugural meeting in January 2026 but still lacks a statutory foundation – transforming it into one coherent statutory forum for coordination.

Membership: Reflecting the current distribution of EU digital governance, EDPS and EDPB would cover data; the European Board for Digital Services (EBDS) would cover platforms; the DMA High-Level Group would cover digital gatekeepers; the AI Board would cover AI; ENISA cybersecurity; BEREC connectivity; ECN competition policy; and the Joint ESA Committee the digital finance dimension. As the Commission currently holds enforcement authority over gatekeepers, VLOPs / VLOSEs, and GPAI models, it would chair the EU DRCF without voting rights – a transitional arrangement that explicitly anticipates the gradual transfer of those enforcement responsibilities away from the politicised institution. The EDPS would serve as secretariat, minimising costs while leveraging existing infrastructure and expertise. The Fundamental Rights Agency (FRA) and Europol would participate as observers. Since the EU DRCF absorbs rather than competes with existing structures and creates no new leadership positions beyond the EDPS's existing secretariat function, it would neither face significant institutional resistance nor trigger appointment controversies.

Powers and functions: The new coordination mechanism covers the full breadth of the digital rulebook. Core functions include systematic information sharing across sectoral boundaries; early identification of cross-regulatory tensions before contradictory outcomes emerge; development of

[3a] Could be introduced together with the Digital Fitness Check, which is planned for Q1 2027.

joint guidance and shared methodologies; and coordination on complex cross-border cases. The UK DRCF offers a useful indication of what tangible outputs look like in practice. Now in its sixth year, it publishes an annual workplan setting out joint priorities across its member regulators (i.e. FCA, ICO, Ofcom, and CMA).[36] Its horizon scanning function has produced concrete regulatory impact: previous work on quantum computing directly influenced recommendations for its regulation. The 2026/27 workplan extends this to agentic AI systems, cybersecurity, open finance, and smart data; all areas where cross-regulatory coherence matters precisely because no single regulator has full jurisdiction. In the longer term, the EU DRCF would provide the platform for our broader reform vision (Step Three): consolidated independent enforcement bodies for AI, data, platforms, cybersecurity, connectivity, and competition aligning as equals rather than from within disconnected policy silos of an increasingly politicised European Commission.

International dimension: Through the established International Network for Digital Regulation Cooperation (INDRC), which brings together governance coordination forums from the UK, Netherlands, Ireland, Australia, and Canada, the EU DRCF could immediately access a vibrant global knowledge-sharing network.

Figure 7: Step One – An EU Digital Regulation Cooperation Forum (EU DRCF)

Limitations and political viability: The EU DRCF alone cannot close the enforcement gap. It lacks binding authority and it cannot neutralise the geopolitical trap or overcome resource asymmetries. There is also the risk of creating inherent limitations if the mandate is not clear enough and resources are lacking. Yet, these limitations do not undermine the case for our Step One. Such a coordination body could play an important role in building institutional trust and demonstrating value to make a sufficient case for deeper integration. Even its failure would provide important insights: revealing where independent enforcement capacity is indispensable. At the same time, its political feasibility is strong. Influential member states already operate national equivalents (e.g. Netherlands' Digital Regulation Cooperation Platform, Ireland's Digital Regulators Group), making principled opposition to an EU-level counterpart difficult to sustain. Further, two current attempts at looser or narrower cooperation arrangements (i.e. Germany's Digital Cluster and France's DSA-specific tripartite agreement) provide additional cautionary examples. Operating through published outputs and transparent procedures, the EU DRCF satisfies the Meroni ruling without requiring further institutional isolation from the political process. With the EDPS secretariat infrastructure already in place and no EU treaty change required, a 2027 launch – proposed by the Digital Fitness Check in Q1 2027 and set up by the Commission – is feasible.

Step Two: Create an EU DEA to enforce against widespread infringements

For the medium term, the solution lies in repurposing existing structures rather than creating new EU governance structures from scratch. The best pick is therefore the European Health and Digital Executive Agency (HaDEA), set up in early 2021 to group health, digital, industry, and space-related implementation programmes in one executive agency.

Why HaDEA? It is not likely to persist in its current form beyond the 2021–2027 EU budget. Executive agencies tend to transform with every new MFF due to new priorities and programmes by the Commission and its own annual activity report from 2024 already laments the challenges of managing such a diverse and complex portfolio simultaneously.[44] Compared to existing decentralised EU agencies (like ENISA or the BEREC Office), HaDEA has no entrenched mandate, no specialist constituency defending its current form, and no member state coalition with strategic

interest in preserving its portfolio. What HaDEA does have is operational infrastructure: physical premises in Brussels, established HR procedures, a functioning accounts and audit structure, and – critically – staff with existing working relationships with both the Commission and member state counterparts. The secretariat and operational backbone also do not need to be built from scratch. And finally, HaDEA today is no stranger to mandate transformation. It implemented health and food safety policy from 2005, absorbed consumer and agriculture portfolios in 2014, and then swapped food safety and consumer for digital, industry, and space when it transformed into HaDEA in 2021.

And why now, ahead of the 2028-2034 MFF? The MFF negotiation cycle is the single most important window in EU institutional politics and it only opens every seven years. New bodies proposed outside MFF negotiations face the full weight of "new EU body" criticism – budgetary, political, and constitutional – without the covering logic of a broader institutional rationalisation. Embedding a DEA transformation within MFF negotiations frames it instead as a reallocation of existing commitments and as a rationalisation of EU institutional architecture. Acting now, in the preparatory phase of MFF negotiations, means the DEA concept can be shaped into the Commission's MFF proposals rather than retrofitted.

There's also a statutory argument that aligns with the chosen timing: Article 112 of the AI Act requires the Commission to evaluate by August 2028 whether the AI Office has sufficient powers and resources, and by August 2029 whether a dedicated Union agency is needed to resolve enforcement shortcomings. Both reviews will land in the early implementation phase of the next MFF. Positioning the DEA transformation within the current MFF negotiations means that when the evaluation reports arrive, a concrete and comprehensive institutional proposal – spanning AI, data, and platforms – is already on the table, rather than the reviews themselves requiring a hasty, narrower proposal from scratch and outside the MFF negotiation window. Our blueprint for creating such a Digital Enforcement Agency (DEA) is as follows:

Set-up and legal base: The EU should leverage the institutional foundation of HaDEA and use the upcoming 2028–2034 MFF to transform it into a DEA. Its current diverse set of programmes could be relocated across other relevant executive agencies, as was done with previous MFFs.

The transformation into the DEA would require two legislative steps: a founding act under Article 114 TFEU – the most plausible available legal basis[56] converting HaDEA from an executive agency into a decentralised EU agency with enforcement powers against private parties;[4a] and targeted amendments to the relevant digital laws (i.e. DMA, DSA, AI Act, GDPR, Data Act) transferring enforcement competences from the Commission and, for certain cases, from national competent authorities to the DEA.

The Meroni Doctrine does not block this path. The ECJ established in its Short Selling judgment[27] – as subsequently confirmed by AMLA's establishment in 2024 – that bounded discretion satisfies constitutional requirements, provided enforcement powers are technically defined, objectively triggered, and fully reviewable.[32] A DEA operating on this basis would derive legitimacy from accountability rather than institutional separation.

Scope and organisational structure: Even within digital, the DEA's jurisdiction should be deliberately scoped. Well-performing structures already exist for cybersecurity (ENISA), connectivity (BEREC), and – under the broader reform vision outlined in Step Three – competition. The DEA's mandate should therefore focus on the intersection where enforcement failures are most acute and governance most fragmented: AI, data, and platform regulation.[45] Concretely, this means the AI Act, DMA, DSA, and – for cross-border cases where national enforcement has broken down – the Data

[4a] According to Council Regulation (EC) No 58/2003, executive agencies are limited in managing EU programme budgets and cannot exercise enforcement powers against private parties. A founding act is therefore legally necessary.

Act[5a] and the GDPR[6a]. While some have argued that the DMA and AI Act frameworks are not yet sufficiently stable for enforcement delegation,[33] the DEA's scoping for the 2028–2034 MFF period directly addresses this timing objection: by that point the relevant parts of the AI Act will have been in force for two years and the DMA enforcement architecture will be substantially more settled.[34]

For institutional and political reasons, the Commission would retain its policy and designation functions – determining who qualifies as a gatekeeper, VLOP or VLOSE, and which GPAI models trigger systemic risk obligations – as well as the power to formally determine that national enforcement has demonstrably failed, thereby triggering DEA jurisdiction for specific cross-border GDPR and Data Act cases. The DEA would only assume downstream technical enforcement: investigations, audits, inspections, and the imposition of fines and remedies. This deliberate separation of designation from enforcement insulates technical enforcement decisions from the policy-level decisions over the scope of the rules.[16] In this new governance system, national competent authorities would also retain primary jurisdiction for domestic cases; the DEA's competence is strictly triggered by cross-border dimension, Union-wide systemic risk, or – for GDPR and Data Act cases – a formal Commission determination that national enforcement has broken down, with a clear allocation mechanism built into the founding act to prevent forum shopping.

Figure 8: Step Two – A Digital Enforcement Agency (DEA)

LEGAL BASE	Founding act under Article 114 TFEU converting HaDEA into a decentralised EU agency. Targeted amendments of relevant laws, transferring enforcement competences.
SCOPE	AI, data, and platform regulations (AI Act, DMA, DSA and - for cross-border cases where national enforcement has broken down - the Data Act and the GDPR).
STRUCTURE	Four enforcement domains: (1) gatekeeper conduct, (2) systemic risk and online safety, (3) GPAI models and data processing, and (4) democratic integrity. Overall 450–500 staff with roughly 70-80% redeployed from Commission units.
POWERS	Own-initiative investigations, audits and inspections · joint supervisory teams with national authorities · fines and remedies decided by an independent executive board. Designation of gatekeepers etc. stays with the Commission.
SAFEGUARDS	Non-political leadership appointments · fee-based funding the Commission cannot unilaterally reduce · Board of Appeal + full judicial review.

Rather than organising by legislation – which would replicate the fragmentation the DEA is designed to overcome – the new agency should structure around four enforcement domains: gatekeeper conduct and market contestability, systemic risk and online safety, GPAI models and data processing, and democratic integrity.

Its size should reflect both the total number of designated companies under supervision and their overlap across domains. The net total of unique companies under the DEA's supervision would start with 20-24 companies (with variance for the AI Act), but the gross number would be almost double, as most companies fall under multiple domains of supervision. At least five companies will fall under all four domains. To size accordingly, the DEA should accommodate this overlap by mirroring AMLA's 10:1 ratio of staff to supervised entities[16] for each domain, to ensure enough dedicated staff for adequate supervision of each entity. Applying this ratio to the number of entities (real and estimated) under each domain, a starting size of 450-500 total is realistic (see Figure 9). Of this total, however, only 20-30% would need to be freshly recruited: roughly 350 could be drawn from the Commission's DSA, DMA, and AI Act enforcement units (planned, not current, figures), save for those conducting policy and designation work, and an additional 100-150 could then be recruited from member states, civil society, and industry.

The European Centre for Algorithmic Transparency (ECAT), which is currently housed within the Commission's Joint Research Centre and already supports DSA enforcement through scientific and technical expertise, could provide a ready-made and inhouse knowledge base for the AI and platform enforcement domains.

[5a] The DEA's residual Data Act competence would be limited to large data processing service providers under the Articles 23–31 cloud-switching and interoperability rules, and only where cross-border systemic failure is demonstrable.

[6a] Rather than transferring cross-border GDPR competence wholesale, the DEA should intervene only where the lead DPA demonstrably fails under the one-stop-shop mechanism, mirroring the EBA's Article 17 breach-of-Union-law powers.

Figure 9: Breaking down the envisioned staff size for an EU DEA

Domain	Instrument	Companies supervised	Companies overlapping domains	Target staff size, 10:1 staff to companies
Gatekeeper conduct and market contestability	DMA	7	7 (all gatekeepers are also VLOPs / VLOSEs)	70
Systemic risk and online safety	DSA	~17-18	7-8 (gatekeepers + X, TikTok also fall under democratic integrity)	180
GPAI models and data processing	AI Act, Data Act, GDPR	~10-14	8-10 (all gatekeeper affiliated companies + OpenAI, Anthropic, Mistral)	140
Democratic integrity	DSA (subset), GDPR (subset)	~7-8	7-8 (entirely a subset of DSA; most are also DMA gatekeepers)	80

Powers and functions: The structural logic of delegating enforcement to the DEA goes beyond mere independence. When enforcement is delegated to an independent agency, the Commission is largely absolved of the geopolitical pressure that currently accompanies it – removing the leverage that powerful foreign governments and companies have over EU regulatory decisions. A game-theory analysis of the current geopolitical trap illustrates why this matters: once enforcement is structurally insulated from political will, without a political actor capable of capitulating, retaliation offers no strategic payoff and becomes irrational to pursue.[46] The EU's commitment to enforcement becomes more credible, precisely because it is no longer discretionary.

Operationally, the DEA would open investigations on its own initiative or upon referral from national competent authorities or the Commission. The agency would also have autonomous powers similar to national data protection authorities. It could request information, conduct inspections, summon and interview persons, and audit compliance. Day-to-day supervision of designated entities (e.g. gatekeepers, providers of systemic GPAI models) would be carried out by joint supervisory teams combining DEA staff with seconded national competent authority officials – a structure modelled on AMLA's joint supervisory teams – ensuring that national expertise backs up European enforcement. Final infringement decisions and the imposition of fines would rest not with the Commission, but with the DEA's executive board. This executive board could follow AMLA's model and be composed of a chair, appointed by the Council after the European Parliament's approval on a Commission shortlist; five full-time members including a vice chair, appointed through the same procedure on the basis of expertise across the relevant regulatory domains and with no two members from the same member state; a Commission representative without voting rights, and an executive director appointed by the executive board itself, responsible for day-to-day management.

Learning from the GDPR's years-long proceedings, the DEA's founding act should fix statutory deadlines for each stage of the enforcement process – opening a case, completing an investigation, issuing preliminary findings, adopting final decisions – modelled on the 12- to 15-month timeframes that the 2025 procedural rules introduced for GDPR cross-border cases. Yet, deadlines without consequences invite exactly the kind of drift the current system already displays. Deadlines should therefore carry automatic escalation triggers – a missed deadline would require mandatory notification to the DEA's independent oversight board and, if unresolved within a further fixed period, an accelerated referral to the Board of Appeal, empowered to set a binding completion date or, in cases of unjustified delay, refer matters directly to a dedicated digital chamber of the General Court.

Beyond its core investigative and sanctioning powers, the DEA should – already at launch – carry a second mandate addressing one of the structural vulnerabilities identified above: knowledge preservation. The DEA would publish annual enforcement priorities and horizon scanning assessments of emerging technological risks – a practice established by ESMA through its annual work programmes and risk heatmaps – feeding analysis and insights into the EU's policy cycle. A third mandate, democratic resilience, should be added only once it rests on a firmer legal footing. The DEA's founding act should therefore contain a review clause – similar to Article 112 of the AI Act – requiring the Commission to assess, by 2030, whether to extend the DEA's competences to the enforcement of democratic-resilience obligations, conditional on a binding legal basis being in place. At present the 'Centre for Democratic Resilience' – launched in February 2026 under the European Democracy Shield – operates as a voluntary coordination hub with early-warning and information sharing functions but no enforcement powers. A dedicated mechanism flowing from the Democracy Shield could supply the substantive obligations against information manipulation and synthetic media that the DEA could then enforce. Once such a legal basis exists, the DEA could absorb the Centre's operational functions, establish an independent early-warning capability, and cooperate with law enforcement and – where the Commission has formally determined foreign-state direction – impose operational restrictions on platforms interfering systemically in European democracy.[47]

The EU DRCF – from Step One – would serve as the permanent coordination platform between the DEA and the surrounding regulatory ecosystem (especially ENISA and BEREC), ensuring that enforcement in other digital fields remains coherent with the DEA's activities.

Independence and accountability: The DEA's independence must be structural, resting on four mutually reinforcing mechanisms – leadership appointment, funding autonomy, judicial accountability, and expertise integrity.

First, leadership: The candidate who becomes chair of the DEA Executive Board should be proposed by the Commission, scrutinised by the European Parliament, and formally appointed by the Council not only for democratic rigour, but also for political armour to ensure the independence of the role. Persons currently holding political mandates or senior Commission positions (i.e. head of unit or higher) should be explicitly excluded to pre-empt the appointment controversies that have undermined other EU bodies.[48] Instead, each candidate must have longstanding experience in enforcing laws with at least six years in a related national leadership position. Terms are fixed at five years and renewable once. A removal from office is only permitted in case of serious misconduct or if the person suddenly fails to meet the conditions necessary for the duties.

Second, funding: The DEA requires dedicated budget lines that the Commission cannot unilaterally reduce. These should be supplemented by supervisory fees levied on companies within the agency's jurisdiction: the DSA supervisory fee (= currently 0.05% of global annual net income from VLOPs and VLOSEs[49]) already exists and should be redirected from the Commission budget to the DEA. As supervisory fees could then be used to fund enforcement of the respective digital rulebook, they should be added where absent or increased where present. This fee-based income is constitutionally significant: a decentralised EU agency that cannot be starved of resources through budget pressure is structurally harder to capture than one dependent on annual appropriations – a lesson drawn directly from the design of ESMA and AMLA.[33]

Third, accountability: All decisions taken by the DEA should be subject to an internal Board of Appeal as first-instance review, followed by judicial review before the General Court with appeal to the Court of Justice. This would ensure that the full accountability chain matches the standard that was established for ESMA and AMLA.[50] A dedicated digital chamber of the General Court for digital enforcement cases – analogous to the IP chamber – would reduce case queue times and build specialised judicial expertise. Ultimately, this dedicated appeals chamber would speed up appeals processes, reducing vulnerabilities for exploitation by powerful tech companies. An independent oversight board publishing regular assessments of enforcement effectiveness as well as mandatory parliamentary hearings for the DEA's chair round out the accountability architecture. However, it

should be acknowledged that the combination of significant enforcement powers, limited Commission oversight, and the CJEU as ultimate accountability layer still creates a constitutional tension that the DEA's design mitigates but does not fully resolve.[51] This points toward long-term treaty-level reforms that Step Three of our digital governance reform will ultimately require.

Fourth, expertise integrity: the DEA should operate under binding restrictions on which external experts and consultancies it may draw on. Any external advisor should disclose current and past commercial relationships with designated companies on a standing register, with a cooling-off period before advising on a matter touching a former client. A substantiated conflict-of-interest complaint should trigger a hearing before the DEA's independent oversight board, with recourse to the Board of Appeal where a complaint is rejected.

Political viability: While the transformation of an existing structure reduces political resistance, it does not eliminate it. Three specific interests will push back: the Commission, which loses enforcement powers and associated budget; well-resourced national competent authorities, which lose jurisdiction over cross-border cases they currently handle; and certain tech companies, which benefit from the enforcement fragmentation and will resist a more capable, depoliticised enforcement body.[52] Resistance from fiscally conservative member states is a further structural obstacle – any proposal that expands the EU institutional architecture, even through transformation rather than creation, will face budgetary scrutiny from this group.[53]

Three design choices directly address these obstacles. First, the HaDEA transformation model significantly reduces the 'new EU body' objection that has historically triggered opposition: the institutional shell of HaDEA already exists, the staff transfers rather than is recruited from scratch, and the MFF negotiation cycle embeds the proposal within a broader budgetary rationalisation rather than exposing it to isolated political opposition. Second, the non-political leadership condition is not only an accountability mechanism but an indispensable precondition for assembling the cross-party coalition that Step Two requires. An agency whose chair is selected on merit rather than political affiliation furthermore directly pre-empts the appointment controversies documented above, removing one of the most reliable political weapons against new EU bodies.[54] Third, large tech companies may ultimately find that the greater legal certainty and predictability that technically bounded, depoliticised enforcement provides outweigh their resistance – compared to the current Commission model, where enforcement is subject to geopolitical and industrial policy pressures.

Against these obstacles, the case for the DEA is grounded in documented failure. The Commission's own enforcement record – its staggered DMA decisions under US trade pressure,[12] its 76% staffing shortfall for DMA supervision, and its structural inability to act simultaneously as industrial policy actor and impartial digital enforcer – provides the empirical foundation for change across all five structural weaknesses identified above (see Figure 3): geopolitical vulnerability, politicised enforcement, fragmented governance, capacity shortfalls, and national protectionism. No existing proposal managed to address all five simultaneously. The DEA, proposed in this paper, does.

Figure 10: The enforcement gap – could a sequenced reform overcome it?

	Step 1: EU DRCF	Step 2: EU DEA	Step 3: Long-term governance reform
Geopolitical Capture	No	Yes	Yes
Accountability Deficit	Partially	Largely	Yes
Governance Fragmentation	Partially	Largely	Yes
Resource Gaps	Partially	Largely	Yes
National Interests	No	Yes	Yes

Figure 11: Legal & political hurdles – could a sequenced reform overcome them?

	Step 1: EU DRCF	Step 2: EU DEA	Step 3: Long-term governance reform
Meroni Doctrine	Yes	Yes	Yes, with unanimous political support
Institutional Resistance	Yes	Yes, with political support	Yes, with significant political support
Fiscal and Political Backlash	Yes	Yes, with political support	Yes, with significant political support
Leadership Appointments	Yes	Yes	Yes

Step Three: Long-term treaty-level governance reforms

The EU DRCF and the DEA attempt to close the enforcement gap within the boundaries of the current EU Treaties. Yet, those boundaries themselves remain part of the overall problem. As this paper has argued throughout, the EU's institutional architecture – designed for a Commission that legislates, member states that implement, and courts that review – does not naturally accommodate powerful independent enforcement bodies that operate across the entire Digital Single Market. Steps One and Two work within this architecture. Step Three goes further and proposes to change it.

The constitutional tensions existing today are structural. The ECJ's Short Selling judgment[27] and AMLA's establishment demonstrate that the current Treaties can accommodate bounded delegation. However, critics such as Simoncini argue that this amounts to a judicial blessing of de facto constitutional evolution rather than a proper democratic choice.[51] For AMLA specifically, the combination of no Commission instruction power, direct sanctions against private entities, and a legal basis in Article 114 TFEU not designed for permanent supervisory bodies creates what might be called a legitimacy gap alongside the enforcement gap.[56] Although formal management boards and parliamentary hearings can mitigate it, they – with the CJEU as the only apex of the accountability pyramid – do not fully resolve it.[57] A treaty revision would allow the EU to do explicitly what secondary law over the past decades has been doing implicitly: authorise a fully independent enforcement mechanism with direct sanctions powers, clear accountability chains to the European Parliament, and legal bases designed for permanent supervisory institutions rather than adapted from internal market harmonisation.[16]

Figure 12: Step Three – EU Treaty-level reform

MECHANISM	EU Treaty revision: explicit legal bases for fully independent enforcement agencies with direct enforcement powers and clear accountability mechanisms.
VISION	A four-pillar enforcement architecture for the Digital Single Market: DEA (AI, data & platforms) · strengthened ENISA (cybersecurity) · reformed BEREC (connectivity) · independent EU Competition Authority.
GOVERNANCE	The EU DRCF evolves from advisory forum into the permanent platform coordinating these independent enforcement bodies as equals.
THRESHOLD	Unanimous agreement among member states and ratification across twenty-seven constitutional orders.

What such a revision could unlock is a full four-pillar enforcement architecture for the entire Digital Single Market. The DEA would cover AI, data, and platforms. A strengthened ENISA would assume direct enforcement of all cybersecurity laws rather than coordination alone. A reformed BEREC would acquire genuine enforcement powers over connectivity frameworks. An independent EU Competition Authority – separating DG COMP's decision-making function from the Commission – would complete the architecture. More broadly, a genuinely complete institutional architecture would extend the same logic to digital regulation in the media and finance sectors, creating treaty-grounded independent EU agencies in both domains as

well. The EU DRCF, established in Step One, would evolve from a cooperation forum into the permanent governance platform that coordinates these different governance bodies as equals. This would be, in fact, the EU equivalent of the UK's DRCF model but with genuine enforcement teeth across the entire digital economy.

Whether such treaty reform is politically achievable is an open question. It requires unanimous agreement among all EU member states and ratification across twenty-seven constitutional orders; a threshold that has made treaty revision a thing of the past. However, the trajectory is already pointing in this direction. The Digital Decade framework, the Draghi and Letta reports, and the growing consensus around the need for an enforcement reform all point toward an institutional architecture that the current EU Treaties cannot fully support.[58] [59] Commission President Ursula von der Leyen has also repeatedly called for treaty change.[60] In this regard, the paper sees Steps One and Two not merely as interim measures. On the contrary, both of them are the political and institutional preparation for the deeper transformation that Step Three would entail.

Conclusion: A sequenced approach to close the EU enforcement gap

This sequenced approach recognises political realities while building and maintaining reform momentum. In the short term, the EU DRCF builds trust, develops shared methodologies, and demonstrates concrete value. In the medium term, HaDEA's transformation into the DEA, and, in the long term, treaty-level reforms deliver independent EU enforcement capacity that European digital sovereignty and competitiveness ultimately require.

Each step is necessary but insufficient alone – their logic is cumulative and they must be read as a strict sequence. Coordination without independent accountability capacity leaves the structural deficits unresolved. Independent accountability capacity without prior coordination lacks the political and cultural foundations for success. And singular institutional reform without treaty-level reform risks locking in a hybrid architecture at the Digital Single Market level, reproducing the very fragmentation it sought to overcome. Taken together, the three steps chart a realistic path from the EU enforcement gap today toward the credible, effective digital governance that European citizens and businesses deserve.

Authors

Kai Zenner is the Head of Office and Digital Policy Adviser of MEP Axel Voss at the European Parliament, Member of OECD/WEF AI Expert Groups, and Fellow of Practice at the TUM Think Tank. All expressed views are personal and do not represent the position of the European Parliament.

Maria Koomen is a democracy and tech analyst, public-interest advocate, and civic educator.

This Strategy Note benefited from helpful discussions with a number of EU digital policy and governance experts. Many thanks in particular to Mark Dempsey, Julian Jaursch, Laura Lazaro Cabrera, Helena Malikova, Mario Mariniello, Zach Meyers, Johnny Ryan, Max von Thun, and Cindy Zheng. It also enjoyed design work by Philipp Kienemund – thanks, Philipp!

Notes

1 “A dataset of EU legal and policy instruments for the digital world,” Kai Zenner, J. Scott Marcus, and Kamil Sekut, Centre for European Policy Studies (CEPS), July 2025, https://cdn.ceps.eu/2025/08/CEPS-Zenner-Dataset-July-2025.pdf.

2 “Enforcement Is Crucial for EU’s Tech Policy Success,” Maria Koomen and Raegan MacDonald, Centre for Future Generations, 23 July 2024, https://cfg.eu/enforcement-is-crucial-for-eus-tech-policy-success/.

3 “The Future of European Competitiveness,” Mario Draghi, European Commission, 9 September 2024, https://commission.europa.eu/topics/competitiveness/draghi-report_en.

4 “Irish DPC handles 99.93% of GDPR complaints, without decision?,” None of Your Business (noyb), 28 April 2021, https://noyb.eu/en/irish-dpc-handles-9993-gdpr-complaints-without-decision.

5 “Opening statement to the Joint Justice Committee,” Johnny Ryan, Irish Council for Civil Liberties (ICCL), 24 March 2026, https://data.oireachtas.ie/ie/oireachtas/committee/dail/34/joint_committee_on_justice_home_affairs_and_migration/submissions/2026/2026-03-24_opening-statement-dr-johnny-ryan-director-of-enforce-irish-council-for-civil-liberties_en.pdf.

6 “Annual Report 2024: Protecting Personal Data in a Changing Landscape,” European Data Protection Board, April 2025, https://www.edpb.europa.eu/system/files/documents/2025-04/edpb-annual-report-2024_en.pdf.

7 “EU Digital Policy in 2025: From the loss of orientation to reclaiming European leadership in the Age of AI,” Paul Nemitz, Foundation for European Progressive Studies (FEPS), January 2026, https://feps-europe.eu/wp-content/uploads/2026/01/10.-EU-digital-policy-in-2025.-From-the-loss-of-orientation-to-reclaiming-European-leadership-in-the-age-of-AI.pdf.

8 “Much More Than a Market,” Enrico Letta, Council of the European Union, April 2024, https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf.

9 “Escaping the simplification trap: A playbook for the EU’s digital rulebook,” Kai Zenner, *Computer Law & Security Review*, Volume 60, April 2026, https://www.sciencedirect.com/science/article/abs/pii/S2212473X25001178.

10 “The von der Leyen Commission: for a Union that strives for more,” press release, European Commission, September 2019, https://ec.europa.eu/commission/presscorner/detail/en/ip_19_5542.

11 “EU Tech Chiefs Say They Don’t Target US Tech,” Politico Europe, 7 March 2025, https://www.politico.eu/article/eu-tech-chiefs-say-they-dont-target-us-tech/.

12 “Big Tech Fines Just Got Political, Whether the Commission Likes It or Not,” Politico Europe, 14 April 2025, https://www.politico.eu/article/big-tech-fines-digital-markets-act-political-european-commission-meta-apple-donald-trump-tariffs/.

13 “Over 30 Civil Society Orgs Express ‘Grave Concern’ About Von der Leyen’s Reported Google Backdown,” press release, Open Markets Institute Europe, 6 May 2026, https://www.openmarketsinstitute.eu/publications/orgs-express-grave-concern-about-von-der-leyens-reported-google-backdown.

14 “EU Regulation and Institutions for Digital Competitiveness,” Alexandre de Streel and Zach Meyers, Centre on Regulation in Europe (CERRE), November 2025, https://cerre.eu/wp-content/uploads/2025/11/EU-Regulation-and-Institutions-for-Digital-Competitiveness.pdf.

15 “Big Tech Lobby Budgets Hit Record Levels,” Corporate Europe Observatory, October 2025, https://corporateeurope.org/en/2025/10/big-tech-lobby-budgets-hit-record-levels.

16 “The case for a European Union digital enforcement authority,” Mario Mariniello, Bruegel, 5 March 2026, https://www.bruegel.org/policy-brief/case-european-union-digital-enforcement-authority.

17 “Simplifying the EU Digital Rulebook: Clarity, simplicity, and agility for competitiveness,” BusinessEurope, July 2025, https://www.businesseurope.eu/wp-content/uploads/2025/07/2025-07-17-BusinessEurope-Paper-Simplification-of-the-Digital-Rulebook.pdf.

18 “Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR),” European Data Protection Board, 13 April 2023, https://www.edpb.europa.eu/system/files/2023-05/edpb_bindingdecision_202301_ie_sa_facebooktransfers_en.pdf.

19 “The Italian Data Protection Authority Halts ChatGPT’s data processing operations,” Clifford Chance, 6 April 2023, https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2023/04/the-italian-data-protection-authority-halts-chatgpt-s-data-proce.html.

20 “Doubling Down, Not Backing Down: Defending the EU’s Digital Sovereignty in the Trump Era,” Max von Thun, Georg Riekeles, and Pencho Kuzev, Konrad-Adenauer-Stiftung, February 2025, https://www.kas.de/en/monitor/detail/-/content/durchsetzen-statt-nachgeben.

21 “Enforcing EU law – The Commission has improved its management of infringement cases, but closing them still takes too long,” Special report 28/2024, European Court of Auditors, 17 December 2024, https://www.eca.europa.eu/en/publications/SR-2024-28.

22 “Creating the space for competitive and resilient digital Europe,” Johnny Ryan, Felix Kartte, and Pencho Kuzev, Konrad-Adenauer-Stiftung, November 2024, https://www.kas.de/documents/252038/29391852/Creating+the+Space+for+Competitive+and+Resilient+Digital+Europe.pdf/.

23 Based on bilateral conversations of the authors of this piece with EU officials. Some elements of this idea can also be found in academic studies or reports such as the one from the 2019 Commission “Competition Law 4.0” in Germany.

24 “Towards a Digital Clearinghouse 2.0,” European Data Protection Supervisor, 15 January 2025, https://www.edps.europa.eu/system/files/2025-01/towards_a_digital_clearinghouse_2_0_january_2025_en_0.pdf.

25 “A new competition framework for the digital economy,” report by the German Commission “Competition Law 4.0”, German Federal Ministry for Economic Affairs and Energy, September 2019, https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Publikationen/Wirtschaft/a-new-competition-framework-for-the-digital-economy.pdf?__blob=publicationFile&v=2.

26 “Competition Policy and Industrial Policy: For a reform of European law,” Bruno Deffains, Olivier d’Ormesson, and Thomas Perroud, Robert Schuman Foundation, 20 January 2020, https://www.robert-schuman.eu/en/european-issues/0543-competition-policy-and-industrial-policy-for-a-reform-of-european-law.

27 “The 2014 ESMA ‘Short Selling’ judgment (Case C-270/12),” Court of Justice of the European Union, 22 January 2014, https://curia.europa.eu/site/upload/docs/application/pdf/2014-01/cp140007en.pdf.

28 “Charting a European Path to Competitiveness,” Zach Meyers, Alexandre de Streel, and Antonio Manganelli, Centre on Regulation in Europe (CERRE), 8 January 2026, https://cerre.eu/publications/charting-a-european-path-to-competitiveness/.

29 “The DSA Draft: Ambitious Rules, Weak Enforcement Mechanisms,” Julian Jaursch, interface (formerly Stiftung Neue Verantwortung), 25 May 2021, https://www.interface-eu.org/publications/dsa-draft-ambitious-rules-weak-enforcement-mechanisms.

30 “DSA/DMA: Europe Needs to Find Its Own Digital Model,” Renew Europe Group, 25 February 2021, https://www.reneweuropegroup.eu/news/2020-12-15/dsa-dma-europe-needs-to-find-its-own-digital-model.

31 “Digital Services Act: Greens/EFA Successes,” Alexandra Geese MEP, December 2021, https://en.alexandrageese.eu/digital-services-act-greens-efa-successes/.

32 “EU Resolution Framework, Revival of the Meroni Doctrine in the Judgement of the ECJ of 18 June 2024,” Jean-Marc Gollier and Katrien Morbee, Review of European Administrative Law, 6 December 2024, https://realaw.blog/2024/12/06/eu-resolution-framework-revival-of-the-meroni-doctrine-in-the-judgment-of-the-ecj-of-18-june-2024-c%E2%80%91551-22-p-by-jean-marc-gollier-katrien-morbee/.

33 “It is Time for an Independent European Digital Authority,” Mario Mariniello, Bruegel, 30 September 2025, https://www.bruegel.org/first-glance/it-time-independent-european-digital-authority.

34 “Guarding the Gates: The Digital Markets Act and Lessons in Ex Ante Regulation,” William Alan Reinsch and Michael H. Gary, Center for Strategic and International Studies (CSIS), 5 January 2026, https://www.csis.org/blogs/charting-geoeconomics/guarding-gates-digital-markets-act-and-lessons-ex-ante-regulation.

35 “The Digital Services Act Proposal and Ireland,” Ronan Ó Fathaigh, DSA Observatory, 3 December 2021, https://dsa-observatory.eu/2021/12/03/the-digital-services-act-proposal-and-ireland/.

36 “2026/27 Workplan,” Digital Regulation Cooperation Forum, April 2026, https://www.drcf.org.uk/siteassets/drcf/pdf-files/drcf-workplan-2026-27.pdf?v=416509.

37 “Council Conclusions on European Competitiveness in the Digital Decade,” 5 December 2025, https://data.consilium.europa.eu/doc/document/ST-16430-2025-INIT/en/pdf.

38 “‘Grossly understaffed’ EU competition enforcers must prioritize, Guersent says,” Jean Comte, MLex, 8 April 2025, https://www.mlex.com/mlex/articles/2322385.

39 “EU formally opens deficit proceedings against eight member states,” Jack Schickler, Euronews, 26 July 2024, https://www.euronews.com/2024/07/26/eu-formally-opens-deficit-proceedings-against-multiple-countries.

40 “Commission insists Selmayrgate wasn’t a ‘coup’,” Florian Eder, *Politico Europe*, 18 June 2018, https://www.politico.eu/article/martin-selmayr-european-commission-insists-selmayrgate-wasnt-a-coup/.

41 “Romania blocks its own EU prosecutor appointment,” Robert Schwartz, Deutsche Welle, 2 October 2019, https://www.dw.com/en/romania-seeks-to-block-former-anti-corruption-official-from-top-eu-post/a-47446874.

42 “Ombudsman opens inquiry into Commission’s silence on EU privacy chief,” Cynthia Kroet, Euronews, 1 September 2025, https://www.euronews.com/next/2025/09/01/ombudsman-opens-inquiry-into-commissions-silence-on-eu-privacy-chief.

43 “Outrage as Ireland picks ex-Meta lobbyist as new data protection chief,” Owen Carpenter-Zehe, *EUobserver*, 23 October 2025, https://euobserver.com/digital/ar6c78a452.

44 “Annual Activity Report 2024 – Health and Digital Executive Agency,” European Commission, 19 June 2025, https://commission.europa.eu/publications/annual-activity-report-2024-health-and-digital-executive-agency_en.

45 “The Looming Enforcement Crisis in European Digital Policy,” Giovanni De Gregorio and Simona Demková, Verfassungsblog, 10 February 2025, https://verfassungsblog.de/the-looming-enforcement-crisis-ai-dsa-eu/.

46 “Blame shifting and blame obfuscation: The blame avoidance effects of delegation in the European Union,” Tim Heinkelmann-Wild, Bernhard Zangl, Berthold Rittberger, and Lisa Kriegmair, *European Journal of Political Research*, Volume 62, Issue 1, 221–238, 2023, https://doi.org/10.1111/1475-6765.12503.

47 “The European Way. A Blueprint for Reclaiming Our Digital Future,” Kai Zenner et al., 12 May 2025, https://dx.doi.org/10.2139/ssrn.5251254.

48 For more background: Christel Koop and Jacint Jordana, “Regulatory independence and the quality of regulation,” in Martino Maggetti, Fabrizio Di Mascio, and Alessandro Natalini (Eds.), *Handbook of Regulatory Authorities* (pp. 210–226), Edward Elgar, 2022, https://doi.org/10.4337/9781839108990.

49 “EU Commission Gathered 58m in Fees for Supervising Digital Platforms,” Cynthia Kroet, Euronews, 31 March 2025, https://www.euronews.com/next/2025/03/31/eu-commission-gathered-58m-in-fees-for-supervising-digital-platforms.

50 “AMLA and the Common Approach: Rethinking EU Agencification,” Merijn Chamon, Review of European Administrative Law, 19 December 2025, https://realaw.blog/2025/12/19/amla-and-the-common-approach-rethinking-eu-agencification-by-merijn-chamon/.

51 “Eroding Meroni: the Fate of Delegation to EU Agencies,” Marta Simoncini, STALS Research Paper, Sant'Anna Legal Studies, July 2025, https://minisiti.santannapisa.it/app/uploads/sites/21/2025/10/Simoncini_STALS_Meroni-doctrine.pdf.

52 “Mind the trend! Enforcement of EU law has been moving to ‘Brussels’,” Miroslava Scholten, Journal of European Public Policy, Volume 24, Issue 9, 12 May 2017, https://doi.org/10.1080/13501763.2017.1314538.

53 “Rich EU countries set out their red lines ahead of budget negotiations,” Evi Kiorri, *EUobserver*, 17 November 2025, https://euobserver.com/74421/listen-rich-eu-countries-set-out-their-red-lines-ahead-of-budget-negotiations/.

54 “Political Independence, Accountability, and the Quality of Regulatory Decision-Making,” Christel Koop and Chris Hanretty, Comparative Political Studies, Volume 51, Issue 1, 28 March 2017, https://doi.org/10.1177/0010414017695329.

55 “The EU needs an independent competition authority, says top MEP,” Aude Van Den Hove, Politico Europe, 24 February 2025, https://www.politico.eu/article/eu-independent-competition-authority-stephanie-yon-courtin/.

56 “Meroni Circumvented? Article 114 TFEU and EU Regulatory Agencies,” Pieter Van Cleynenbreugel, Maastricht Journal of European and Comparative Law, Volume 21, Issue 1, March 2014, https://doi.org/10.1177/1023263X1402100104.

57 “Follow the Money, AMLA! – How to unleash the EU’s new AML watchdog,” Markus Tiemann, Jacques Delors Centre, 7 October 2025, https://www.delorscentre.eu/en/publications/detail/publication/follow-the-money-amla-how-to-unleash-the-eus-new-aml-watchdog.

58 “Democratizing Draghi: Why the ‘Competitiveness Report’ Demands Treaty Reform,” Peter Lindseth and Päivi Leino-Sandberg, Verfassungsblog, 12 September 2024, https://verfassungsblog.de/draghi-report-investment-eu-competition-treaty-reform/.

59 “Institutional aspects of the Report on the future of European Competitiveness (Draghi Report),” European Parliament, 25 November 2025, https://www.europarl.europa.eu/doceo/document/TA-10-2025-0285_EN.pdf.

60 “Europe’s Choice: Political Guidelines for the Next European Commission,” Ursula von der Leyen, European Commission, 18 July 2024, https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en.

61 “Coded for privileged access: How Big Tech weakens rules on advanced AI,” Corporate Europe Observatory, 30 April 2025, https://corporateeurope.org/en/2025/04/coded-privileged-access.

62 “Spamming the regulator: exploring a new lobbying strategy in EU competition procedures,” Marlene Jugl et al., *Journal of Antitrust Enforcement*, Volume 12, Issue 1, March 2024, https://doi.org/10.1093/jaenfo/jnad009.