



TASK FORCE REPORT

EU LAW AND REGULATION FOR THE DIGITAL WORLD



Rapporteurs

J. Scott Marcus

Artur Bogucki

Jacob Griffith

Chair

J. Scott Marcus

September 2026

CEPS is an independent think tank based in Brussels. Its mission is to produce sound policy research leading to constructive solutions to the challenges facing Europe and the world.

This report reflects the work of a CEPS Task Force on ‘Next steps for EU law and regulation for the digital world’. The Task Force comprised a well-balanced group of experienced policy experts representing industry, academia, and institutions (see Appendix A).

The members deliberated over the course of four full-day hybrid meetings that took place under the Chatham House Rule between January and April 2026. Most of the sessions benefited from opening structuring remarks by highly knowledgeable external experts. Their remarks and presentation materials have added to the report’s findings. A set of principles has guided the entire drafting process, ensuring that the final report is truly multi-stakeholder (see Appendix B). Members also had the opportunity to make written contributions to the report and comment on earlier drafts. The resulting report conveys their valuable input.

The findings and recommendations in this report do not necessarily reflect a common position reached by all members of the Task Force. Nor do they represent, in any manner, the views of their respective institutions. The content of the report and any remaining errors are solely attributable to the rapporteurs.

Suggested citation: Marcus, J. Scott, Bogucki, Artur and Griffith, Jacob (2026), *EU law and regulation for the digital world*, Task Force Report, Centre for European Policy Studies, Brussels.

ISBN 978-94-6138-804-9

© Copyright CEPS 2026

Image credit: www.vecteezy.com

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, mechanical, photocopying, recording or otherwise – without the prior permission of the Centre for European Policy Studies.

CEPS
Place du Congrès 1, B-1000 Brussels
Tel: 32 (0) 2 229 39 11
internet: www.ceps.eu

CONTENTS

EXECUTIVE SUMMARY.....	VI
1. INTRODUCTION	1
2. EXPLOSIVE GROWTH IN THE NUMBER AND COMPLEXITY OF EU ‘DIGITAL’ LAWS.....	4
3. DIGITAL SOVEREIGNTY, OPEN STRATEGIC AUTONOMY, AND INDUSTRIAL POLICY	9
4. COMPETITION AND THE LEVEL PLAYING FIELD: THE DIGITAL MARKETS ACT	12
4.1. IS IT TOO EARLY TO JUDGE EFFECTIVENESS, AND WHAT WOULD SUCCESS LOOK LIKE?	13
4.2. ARE GATEKEEPERS CHANGING THEIR BEHAVIOUR, AND IS COMPLIANCE GENUINE?	15
4.3. ENFORCEMENT CLARITY, COMPLIANCE KPIS, AND THE LIMITS OF DIALOGUE.....	16
4.4. NON-DISCRIMINATION IN DESIGN, DISCRIMINATORY IN EFFECT?	17
4.5. UNINTENDED EFFECTS: PROPORTIONALITY, PRIVACY, SMEs, AND THE INNOVATION TRADE-OFF	18
4.6. INTERACTIONS WITH COMPETITION LAW, OTHER INSTRUMENTS, AND GENERATIVE AI	19
4.7. INSTITUTIONAL ARCHITECTURE: TOWARDS A EUROPEAN SYSTEM OF DIGITAL REGULATORS?	20
4.8. DATA ACCESS AND THE ROLE OF VETTED RESEARCHERS	21
5. FUNDAMENTAL FREEDOMS: THE DIGITAL SERVICES ACT	22
5.1. ENFORCEMENT FRAGMENTATION AND THE DIGITAL SERVICES COORDINATORS.....	23
5.2. MEASURING WHAT MATTERS: TRANSPARENCY AND CONTENT-MODERATION OUTCOMES	24
5.3. AUDIT STANDARDS AND RESEARCHER DATA ACCESS	25
5.4. COMPLIANCE COSTS, SMEs, OVERLAPS, AND DEFINITIONAL SPILLOVER	26
6. THE ARTIFICIAL INTELLIGENCE ACT	27
6.1. THE RISK-BASED APPROACH AND ITS CRITICS	28
6.2. SIMPLIFICATION, GUIDANCE, AND THE SECTORAL DIMENSION	28
6.3. GUIDANCE WITHOUT PRESCRIPTION, AND THE EXPERTISE GAP	29
6.4. GOVERNANCE, STANDARDS, AND THE GENERAL-PURPOSE AI CODE OF PRACTICE	30
6.5. AI AND LIABILITY	30
6.6. SIMPLIFICATION IN PRACTICE: THE DIGITAL OMNIBUS AND THE STREAMLINING OF THE ACT	31
7. PRIVACY, CYBERSECURITY, AND DATA SHARING	33
7.1. PRIVACY: THE GENERAL DATA PROTECTION REGULATION AND DIGITAL OMNIBUS	34
7.2. MEASURES TO IMPROVE THE SHARING OF DATA	38
7.3. CYBERSECURITY	39

8. THE BETTER REGULATION PROCESS: CREATING, EVALUATING, IMPROVING, AND SIMPLIFYING EU LAWS AND REGULATION	44
8.1. <i>EX ANTE</i> IMPACT ASSESSMENT	47
8.2. <i>EX POST</i> EVALUATIONS	51
8.3. SIMPLIFICATION OF THE OVERALL STOCK OF EU LAWS AND REGULATIONS	53
8.4. SINGLE MARKET ASPECTS OF SIMPLIFICATION AND IMPLEMENTATION	57
REFERENCES	61
APPENDIX A. TASK FORCE PARTICIPANTS.....	68
APPENDIX B. PRINCIPLES AND GUIDELINES FOR THE TASK FORCE.....	70

FIGURES

FIGURE 1. CUMULATIVE NUMBER OF EU LAWS DEALING MAINLY WITH DIGITALISATION	7
FIGURE 2. GDPR ENFORCEMENT STAFF SIZE AND BUDGET, SELECTED MEMBER STATES (2020–21).....	36
FIGURE 3. CONCEPTUAL ILLUSTRATION OF THE 2016 INTERINSTITUTIONAL AGREEMENT AS A THREE-LEGGED STOOL: A PROGRESSIVELY WEAKENED PARLIAMENT AND COUNCIL LEAVE THE FRAMEWORK UNSTABLE	47

TABLES

TABLE 1. EU DIGITAL-SECTOR RULES AT A GLANCE.....	6
TABLE 2. COMMISSION PROPOSALS AND ADOPTED ACTS UNDER THE ORDINARY LEGISLATIVE PROCEDURE (2014–24)	7
TABLE 3. DELEGATED AND IMPLEMENTING ACTS UNDER THE ORDINARY LEGISLATIVE PROCEDURE (2014–24)	8

LIST OF RECOMMENDATIONS

RECOMMENDATION 1. THE COMMISSION SHOULD, WITHOUT WAITING FOR THE NEXT REVIEW CYCLE, PUBLISH A CLEAR AND OUTCOME-ORIENTED FRAMEWORK OF INDICATORS FOR CONTESTABILITY, FAIRNESS AND INNOVATION, SPECIFYING THE DATA TO BE COLLECTED. IT SHOULD COMMISSION AT LEAST PART OF THE RESULTING ASSESSMENT FROM A BODY INDEPENDENT OF ITS OWN ENFORCEMENT FUNCTION..... 15

RECOMMENDATION 2. THE COMMISSION SHOULD WORK WITH GATEKEEPERS AND BUSINESS USERS TO STANDARDISE COMPLIANCE REPORTING AROUND AGREED KEY PERFORMANCE INDICATORS FOR PROCESS AND OUTPUT THAT CAPTURE THE ACTUAL UPTAKE OF NEW OPENNESS AND INTEROPERABILITY. IT SHOULD MAKE FULLER USE OF THE SPECIFICATION-DECISION PROCEDURE TO GIVE TIMELY, EXAMPLE-BASED GUIDANCE ON ACCEPTABLE COMPLIANCE AND SHOULD STRENGTHEN THE ROLE OF THE INDEPENDENT COMPLIANCE OFFICER. 17

RECOMMENDATION 3. THE COMMISSION SHOULD EXAMINE WHETHER A BOUNDED DATA-ACCESS MECHANISM FOR VETTED RESEARCHERS, MODELLED ON ARTICLE 40 OF THE DIGITAL SERVICES ACT, COULD SUPPORT INDEPENDENT EVALUATION OF THE EFFECTS OF THE DIGITAL MARKETS ACT ON CONTESTABILITY AND FAIRNESS — SUBJECT TO

STRICT SAFEGUARDS FOR CONFIDENTIALITY AND DATA PROTECTION, AND TO A PROPORTIONATE ASSESSMENT OF THE BURDEN IMPOSED. 21

RECOMMENDATION 4. THE COMMISSION AND MEMBER STATES SHOULD GIVE PRIORITY TO CLOSING THE IMPLEMENTATION GAP FOR THE DIGITAL SERVICES ACT, ENSURING THAT EVERY DIGITAL SERVICES COORDINATOR IS DESIGNATED, SUFFICIENTLY RESOURCED, AND FULLY EMPOWERED. IT SHOULD FORMALLY EVALUATE WHETHER A MORE CENTRALISED ENFORCEMENT BODY, DRAWING ON SECONDED NATIONAL EXPERTISE, WOULD RAISE THE EFFECTIVENESS AND CONSISTENCY OF ENFORCEMENT. THERE IS A NEED NOT ONLY FOR BETTER AND FASTER IMPLEMENTATION, BUT ALSO FOR IMPROVED COORDINATION ACROSS ENFORCEMENT LEVELS. 24

RECOMMENDATION 5. THE COMMISSION, WORKING WITH THE DIGITAL SERVICES COORDINATORS AND THE EUROPEAN CENTRE FOR ALGORITHMIC TRANSPARENCY, SHOULD DEVELOP AND PUBLISH A COMMON SET OF VERIFIABLE OUTCOME INDICATORS FOR CONTENT MODERATION AND SYSTEMIC-RISK MITIGATION, SO THAT COMPLIANCE CAN BE JUDGED ON COMPARABLE EVIDENCE RATHER THAN ON THE PLATFORMS' SELF-DECLARED FIGURES OR ON THE LEVEL OF FINES IMPOSED. 25

RECOMMENDATION 6. THE COMMISSION SHOULD SUPPORT THE DEVELOPMENT OF ADDITIONAL GUIDANCE, CRITERIA, AND BEST PRACTICES FOR THE INDEPENDENT AUDITS REQUIRED UNDER THE DIGITAL SERVICES ACT, BUILDING ON EXISTING ASSURANCE FRAMEWORKS SUCH AS ISAE 3000 (REVISED), WITH THE AIM OF PROMOTING GREATER CONSISTENCY, COMPARABILITY, AND EVIDENTIARY VALUE ACROSS AUDIT ENGAGEMENTS. THE COMMISSION SHOULD ACTIVELY MONITOR THE OPERATION OF THE ARTICLE 40 DATA-ACCESS MECHANISM, STANDING READY TO STREAMLINE THE VETTING AND ACCESS PROCEDURES IF THEY PROVE UNWORKABLE IN PRACTICE FOR BONA FIDE RESEARCHERS. 26

RECOMMENDATION 7. THE COMMISSION SHOULD GIVE PRIORITY TO COMPLETING THE AI ACT'S OVERALL IMPLEMENTING ARCHITECTURE, THE HARMONISED STANDARDS AND PRACTICAL, EXAMPLE-BASED GUIDANCE THAT GIVE PROVIDERS LEGAL CERTAINTY. THERE MAY WELL BE A NEED TO ALSO CLARIFY AI LIABILITY. 32

RECOMMENDATION 8. AMENDMENTS PURSUED UNDER THE SIMPLIFICATION AGENDA SHOULD DISTINGUISH CLEARLY BETWEEN ADMINISTRATIVE STREAMLINING AND SUBSTANTIVE CHANGE. ANY SUBSTANTIVE CHANGE SHOULD BE SUPPORTED BY EVIDENCE AND, WHERE MATERIAL, BY AN IMPACT ASSESSMENT, RATHER THAN JUSTIFIED BY AN UNEXAMINED APPEAL TO URGENCY. 32

RECOMMENDATION 9. THE THREE CO-LEGISLATORS COMMITTED IN 2016 TO JOINTLY IMPLEMENT THE BETTER REGULATION SYSTEM. PARLIAMENT AND THE COUNCIL NEED TO STEP UP TO DO THEIR SHARE IN ORDER TO PROVIDE BETTER CHECKS AND BALANCES WITHIN THE OVERALL BETTER REGULATION SYSTEM. 46

RECOMMENDATION 10. THE COMMISSION SHOULD REDOUBLE ITS EFFORTS TO ENSURE THAT EVERY LEGISLATIVE PROPOSAL IS ACCOMPANIED BY AN IMPACT ASSESSMENT DOCUMENT, EXCEPT IN CASES OF GENUINE URGENCY. IF IT IS TRULY IMPRACTICAL TO PROVIDE AN IMPACT ASSESSMENT WHEN THE LEGISLATIVE PROPOSAL IS SUBMITTED, THE COMMISSION SHOULD, IF POSSIBLE, FOLLOW UP A FEW MONTHS LATER WITH AN ABBREVIATED IMPACT ASSESSMENT. 48

RECOMMENDATION 11. ANY SIGNIFICANT PIECE OF EU LEGISLATION WILL ULTIMATELY DIFFER SUBSTANTIALLY FROM THE INITIAL LEGISLATIVE PROPOSAL SUBMITTED BY THE COMMISSION. LATE IN THE PROCESS BUT PRIOR TO FINAL ENACTMENT, AN ADDENDUM TO THE IMPACT ASSESSMENT SHOULD BE PREPARED TO SUMMARISE THE

DIFFERENCES BETWEEN THE LAW AS PROPOSED AND THE LAW AS ENACTED, INCLUDING AN UPDATE TO THE EXPECTED ADMINISTRATIVE COSTS AND ADAPTATION COSTS. 49

RECOMMENDATION 12. THE *EX POST* EVALUATION TO WHICH ALL SIGNIFICANT PROGRAMMES ARE IN THEORY SUBJECT SHOULD IN FACT BE CARRIED OUT ON A TIMELY BASIS. GOING FORWARD, THE IMPACT ASSESSMENT, AND ULTIMATELY THE LEGISLATION ITSELF, SHOULD ESTABLISH A DEFAULT SCHEDULE FOR SUBSEQUENT EVALUATION; HOWEVER, THIS SHOULD BE DONE IN SUCH A WAY THAT IT DOES NOT PRECLUDE JOINT EVALUATION OF MULTIPLE INTERRELATED MEASURES. 51

RECOMMENDATION 13. THE PROCESS OF EVALUATING LEGISLATION *EX POST* SHOULD NOT BE DONE BY THE COMMISSION. MOVING THE FUNCTION TO, FOR INSTANCE, THE COURT OF AUDITORS, TOGETHER WITH ASSIGNING IT SUFFICIENT STAFF RESOURCES, COULD LEAD TO MORE OBJECTIVE AND IMPARTIAL EVALUATIONS. WHETHER THE COURT OF AUDITORS IS THE MOST APPROPRIATE ENTITY, HOWEVER, WOULD REQUIRE CAREFUL CONSIDERATION. 52

RECOMMENDATION 14. IN ASSESSING THE EFFECTIVENESS OF A LAW, THE *EX POST* EVALUATION MUST CONSIDER WHETHER THE LAW IS ACTUALLY MITIGATING THE PROBLEM FOR WHICH IT WAS CREATED. TO MAKE THAT POSSIBLE, MUCH MORE ATTENTION IS NEEDED WHEN THE IMPACT ASSESSMENT IS DRAFTED TO ENSURE THAT DATA WILL BE COLLECTED THAT ENABLE PROPER SUBSEQUENT EVALUATION. 53

RECOMMENDATION 15. THE ‘ONE IN, ONE OUT’ PRINCIPLE IS GENUINELY IMPORTANT AND PROMISING BUT IT NEEDS TO OFFSET THE ADMINISTRATIVE COST OF A NEW LAW AS ENACTED, NOT JUST THE ADMINISTRATIVE COST OF THE LAW AS INITIALLY PROPOSED. ONE IN, ONE OUT CANNOT HOPE TO FULLY OFFSET THE ADAPTATION COSTS OF THE LAW, WHICH WILL USUALLY BE FAR GREATER THAN THE ADMINISTRATIVE COSTS, BUT IT SHOULD AT LEAST MONITOR THE ADAPTATION COSTS FOR COMPARATIVE PURPOSES. IDEALLY, THE ECONOMIC GAINS FROM THE LAW SHOULD ALSO BE REFLECTED..... 56

RECOMMENDATION 16. THE COMMISSION SHOULD BE MAKING GREATER USE OF THE REFIT PROCESS TO SIMPLIFY EXISTING LAWS SO AS TO REDUCE NEEDLESS REGULATORY COMPLEXITY. 56

RECOMMENDATION 17. THE OMNIBUS PROCESS COULD BE VALUABLE, BUT ITS EFFECTIVENESS HAS BEEN LIMITED TO DATE BY PROCESS DEFICIENCIES IN HOW IT HAS BEEN IMPLEMENTED. SIMPLIFICATION IS BY NO MEANS SIMPLE. PROPER CONSULTATION AND ANALYSIS ARE NEEDED. WHERE CHANGES WITH COMPLEX IMPLICATIONS ARE PUT FORWARD, THE COMMISSION MUST CONDUCT A PROPER IMPACT ASSESSMENT. PURPORTED URGENCY IS NOT AN EXCUSE..... 57

RECOMMENDATION 18. REDUCING FRAGMENTATION REQUIRES A MIX OF MEASURES THAT STRENGTHEN CONSISTENCY IN IMPLEMENTATION AND IMPROVE THE PRACTICAL FUNCTIONING OF THE SINGLE MARKET, WHILE STILL RECOGNISING THAT DECENTRALISED IMPLEMENTATION HAS ITS PLACE. THE EU SHOULD MAKE GREATER USE OF REGULATIONS AND EXPLICIT MAXIMUM HARMONISATION CLAUSES TO LIMIT DIVERGENT NATIONAL INTERPRETATIONS; REINFORCE MEMBER STATE IMPLEMENTATION CAPACITY THROUGH TARGETED FUNDING, TRAINING, AND TECHNICAL ASSISTANCE; AND ENSURE THAT GUIDANCE, TEMPLATES, AND STANDARDISED PROCEDURES ARE AVAILABLE EARLY ENOUGH TO REDUCE THE RISK OF INCONSISTENT NATIONAL APPROACHES. THESE STEPS WOULD NOT ELIMINATE FRAGMENTATION ENTIRELY, BUT THEY WOULD MATERIALLY REDUCE THE GAPS THAT

CURRENTLY ARISE FROM UNEVEN ADMINISTRATIVE CAPACITY, GOLD-PLATING, AND DIVERGENT ENFORCEMENT PRACTICES ACROSS THE MEMBER STATES. 58

RECOMMENDATION 19. THE SOLVIT NETWORK SHOULD BE STRENGTHENED AND MODERNISED SO THAT IT BECOMES A GENUINELY USEFUL TOOL FOR CROSS-BORDER MERCHANTS RATHER THAN A LITTLE-KNOWN MECHANISM USED MAINLY BY INDIVIDUALS. THIS REQUIRES LINKING SOLVIT WITH BUSINESS-FACING ECOSYSTEMS (CHAMBERS OF COMMERCE, ENTERPRISE AGENCIES, AND SECTORAL ASSOCIATIONS), AND IMPROVING STAFFING AND EXPERTISE IN NATIONAL CENTRES – ESPECIALLY FOR DIGITAL-REGULATION CASES. IT ALSO INVOLVES CREATING A CLEARER ESCALATION PATHWAY SO THAT UNRESOLVED OR SYSTEMIC PROBLEMS FEED INTO INFRINGEMENT-PREVENTION MECHANISMS AND THE COMMISSION’S ANNUAL PROGRESS REPORT ON SIMPLIFICATION AND IMPLEMENTATION. GREATER VISIBILITY, MINIMUM CAPACITY STANDARDS, AND A STRUCTURED FEEDBACK LOOP WOULD MATERIALLY INCREASE SOLVIT’S CREDIBILITY AND MAKE IT A MORE EFFECTIVE INSTRUMENT FOR ADDRESSING THE PRACTICAL SINGLE MARKET BARRIERS FACED BY MERCHANTS..... 59

RECOMMENDATION 20. THE SINGLE DIGITAL GATEWAY SHOULD EVOLVE FROM A DOCUMENT REPOSITORY INTO A GENUINELY USABLE COMPLIANCE TOOL FOR CROSS-BORDER MERCHANTS. TO ACHIEVE THIS, SDG CONTENT MUST BECOME EASILY DISCOVERABLE THROUGH SEARCH ENGINES, SUPPORTED BY STRUCTURED METADATA AND MINIMUM QUALITY STANDARDS ACROSS MEMBER STATES. MERCHANTS SHOULD ENCOUNTER CLEAR SUMMARIES, STEP-BY-STEP COMPLIANCE PATHWAYS, AND ALERTS FOR REGULATORY CHANGES RATHER THAN RAW DOCUMENTS ALONE. THE SDG SHOULD ALSO BE LINKED TO SECTOR-SPECIFIC PORTALS AND BUSINESS-ONBOARDING TOOLS, AND ENHANCED WITH ADVISORY FUNCTIONALITY – POTENTIALLY INCLUDING CAREFULLY SAFEGUARDED AI ASSISTANCE – TO HELP USERS IDENTIFY RELEVANT OBLIGATIONS QUICKLY AND RELIABLY. THESE MEASURES WOULD SIGNIFICANTLY INCREASE THE SDG’S VISIBILITY, USABILITY, AND PRACTICAL VALUE FOR BUSINESSES OPERATING IN THE SINGLE MARKET..... 60

EXECUTIVE SUMMARY

CEPS convened a Task Force of knowledgeable industry stakeholders, academic experts, and NGO representatives to think through what is needed to reform and reinvigorate the current and forthcoming EU *digital acquis*. It also considered the process through which EU laws and regulations are designed, implemented, enforced, reviewed, and enhanced over time, with a specific focus on the digital world. This report reflects the Task Force deliberations over the course of four intense, full-day meetings.

The call for reform is timely and widely held to be necessary due to (i) the exploding complexity of EU law and the consequent need for simplification as a means of strengthening EU productivity and competitiveness overall, as highlighted in Draghi (2024b); and (ii) the necessity of strengthening the EU's open strategic autonomy in light of the increasingly tense geopolitical environment and the deterioration of the transatlantic relationship.

In this report, we discuss the explosive growth in the EU digital *acquis* in recent years; the growing importance of open strategic autonomy as it relates to the digital world; key EU digital laws including the Digital Markets Act (DMA), Digital Services Act (DSA), AI Act, General Data Protection Regulation (GDPR); and various cybersecurity measures. We provide detailed recommendations for reform going forward.

Explosive growth in the number and complexity of EU 'digital' laws

Simplification has become a major focus of the current five-year (2024–29) EU legislative mandate, in line with the Draghi report, and this emphasis is appropriate.

In the most recent legislative term, the DMA, DSA, Data Act, AI Act, Data Governance Act, and the Cyber Resilience Act (CRA) were enacted, in addition to broad sectoral measures such as the European Health Data Space (EHDS). These were on top of complex laws already in place, including the GDPR and the European Electronic Communications Code.

This is an acceleration of a long-standing trend. From 2012 to 2024, the number of digital laws grew from 20 to 88; meanwhile, the average length of all EU laws has roughly doubled over the past 20 years. The potential for inconsistencies and tensions among these laws is now beyond the ability of any human expert to assess unassisted.

Some of these laws provide opportunities for EU firms, but all of them impose regulatory burden.

Digital sovereignty, open strategic autonomy, and industrial policy

Reducing the EU's strategic risk in light of growing geopolitical threats and continual tensions in the transatlantic relationship is widely understood to require attention. The change in the transatlantic relationship has been a key driver – the US is the EU's main technology supplier, but it has evolved from a reliable ally to at best a much less predictable actor.

The EU's strategic autonomy goals have not always been clearly articulated – the term *open strategic autonomy* embeds a tension of objectives. The EU has always been strongly committed to global openness, in terms of global value chains and international institutions; however, there are questions as to whether these goals can be fully maintained in the face of worsening global tensions. Global and local value chains are threatened by kinetic war, naval blockades, natural and man-made disasters, high and arbitrary tariffs imposed abruptly for any reason or for no reason, and export controls. International organisations are under great threat and have little or no ability to enforce their decisions. The tension is often expressed as a need to be as open as we can be, while being as closed as we must be.

Nobody is seriously promoting full EU autarky – it is not possible for the EU alone to produce every technology good and service that it needs, just as it is not possible for any region in the world to be entirely self-reliant. But this implies a need for the EU to choose our priorities carefully. Risk assessment is called for, following the classic model of evaluating (i) how likely a risk is to eventuate, (ii) what is the cost if it does, and (iii) what would it cost to guard against the risk. To successfully implement this, we need an in-depth understanding of our dependencies.

In sum, the EU has to strategically defend its interests, increase resilience and supply chain diversity while mitigating threats to value chains, protect intellectual property, and take steps where feasible and where consistent with EU values to retain and expand talent and capital in the EU.

A mix of mitigation measures are likely to be required, aligned with EU values, for critical goods and services: (i) increasing the ability of the EU to self-supply or to provide fall-back solutions for vital sectors; (ii) enhancing resilience by building more diverse and robust international supply chains; (iii) aiming to achieve 'strategic indispensability', where the EU holds leverage in specific niches; and (iv) collaborating more closely with like-minded third countries and trustworthy technology partners. Flanking measures are likely needed to protect intellectual property, and to retain and expand talent and capital in the EU.

Competition and the level playing field: the Digital Markets Act

The DMA has reached the active enforcement phase, with the first specification and non-compliance decisions now taken; yet, it is still early days, and the criteria against which success will be assessed have not been defined in advance.

A key question is whether gatekeepers are genuinely changing their behaviour. The Task Force heard mixed and sharply contested evidence, ranging from documented governance change to allegations of systematic or malicious non-compliance. Again, the criteria for measuring success are not clear.

The DMA was intended to be self-enforcing as much as possible, but it has proven instead to be highly dependent on Commission discretion and dialogue. Gatekeepers and business users alike called for greater clarity, key performance indicators (KPIs) for standardised compliance, fuller use of specification decisions, and better-structured multilateral dialogue. Still, some warned, dialogue has its limits unless backed by enforcement.

The DMA is not discriminatory in design in the sense that its legal provisions do not explicitly discriminate, but the concentration of designated gatekeepers among US firms, and an unfortunate tendency for some policymakers to occasionally refer to the DMA as a form of digital sovereignty, have contributed to a powerful narrative that has fed transatlantic trade tensions. This narrative must be managed if the regime is to endure.

The data needed for rigorous independent evaluation rest almost entirely with the gatekeepers. A more coherent system for European enforcement and a bounded data-access route for vetted researchers (modelled on the DSA) both merit serious consideration.

Fundamental freedoms: the Digital Services Act

The DSA has put in place an ambitious, layered supervisory architecture combining direct Commission oversight of the largest platforms with national Digital Services Coordinators (DSCs), but implementation and enforcement to date have been inconsistent and incomplete. Several Member States were late to designate or fully empower their DSCs, and some have been referred to the Court of Justice.

For the DSA as with other laws, effective enforcement constitutes an essential component of regulatory credibility and compliance. Fines are only one measure of the DSA's success. Meaningful evaluation requires indicators of compliance quality, transparency, and content-moderation outcomes. The instruments to measure these robustly are still ill-defined and immature.

The DSA requires independent audits of very large online platforms. While recognised international assurance standards such as the IAASB's ISAE 3000 (Revised) are already used in practice, there is not yet a dedicated DSA-specific audit standard or commonly accepted audit methodology. This may limit comparability across engagements as well as the evidentiary value of audit outcomes, and likely increases compliance costs.

DSA burdens impact some firms more than others. The heaviest DSA burdens fall on the large firms that provide very large online platforms and search engines; nonetheless, the compliance burdens of the remaining obligations may represent a significant cost for SMEs inasmuch as they have to fund them out of a smaller revenue stream.

The intensifying complexity of EU law overall, particularly as related to the DSA, GDPR and consumer law, together with the growing fragmentation of enforcement, poses compliance risks for firms and creates uncertainty about which regime governs a given situation.

The DSA Article 40 mechanism for vetted-researcher access to platform data is a genuine advance (and potentially a model of best practice that could be applied to the DMA), but its value will depend on whether the vetting and access procedures prove workable in practice.

The Artificial Intelligence Act

The AI Act's risk-based architecture commands broad support in principle, but its operation depends on harmonised standards, guidance and codes of practice that are not yet fully in place, leaving providers unsure how concretely to comply.

The Task Force saw the central challenge not as a binary choice between deregulation and stricter rules, but as a need for practical, example-based guidance that confers legal certainty without becoming over-prescriptive.

As with many of the newer platform regulations, there is a risk that uneven implementation across the Member States might have negative impacts on the EU single market.

The regulators responsible for implementing the AI Act might not always have the necessary operational and technical expertise, and the AI Act itself does not necessarily embody it; moreover, they may have gaps in the complementary expertise, including from the social sciences and humanities, needed to assess its consequences.

The General-Purpose AI Code of Practice and the AI Office are important steps, but the AI governance system remains incomplete with many other building blocks in the making. The 2025–26 simplification effort, through the Digital Omnibus and the related

agreement to streamline the Act, postpones certain obligations and lightens others, but leaves the core requirements substantively unchanged. As with all of the omnibus measures, substantive changes should be grounded in evidence and backed by proper impact assessment.

The lack of an explicit AI liability regime seems to be an issue; however, support for an AI liability pillar is by no means universal.

Privacy, cybersecurity, and data sharing

The GDPR is rightly called Europe's regulatory gold standard. Gold is precious, but it is also heavy.

The Commission submitted a Digital Omnibus ostensibly in an effort to simplify the GDPR. It seeks to simplify cookie rules – as such, a long overdue reform. Yet, the concrete method proposed is challenged by industry stakeholders. The Digital Omnibus also seeks to refine standards for pseudonymisation and to redefine what constitutes personal data, which is a contentious change.

The more fundamental problems in the GDPR – insufficient attention to proportionality, a flawed one-stop-shop approach, and too much complexity overall – remain to be tackled in future legislation. For proportionality, the GDPR contains a single recital, but no operative text to implement it. The problems with the GDPR's one-stop shop (where enforcement mainly falls to the Member State in which a firm has its EU headquarters) are (i) that it saddles two of the smallest Member States with most of the large-scale actions challenging enforcement, and (ii) that the responsible Member State may be subject to a conflict of interest.

Like all omnibus proposals, the Digital Omnibus was put forward without an impact assessment. Parliament is now conducting its own impact assessment.

As is the case for all of the newer EU digital laws, the GDPR is at risk of overlaps and inconsistencies with other EU laws.

The Network and Information Security Directive (NIS 2), the CRA, Digital Operational Resilience Act and forthcoming Digital Networks Act collectively represent the most ambitious attempt yet to build a coherent European cybersecurity architecture in order to reduce systemic vulnerabilities, strengthen resilience, and enhance technological sovereignty. Nonetheless, the current governance model remains fragmented, duplicative, and operationally burdensome. This is particularly so for entities subject to multiple sectoral regimes, due to the accumulated complexity of overlapping obligations, inconsistent definitions, and divergent enforcement practices. Overlaps are especially

prominent between horizontal cybersecurity legislation and sector-specific frameworks, for instance in health, finance, and digital infrastructure.

Aligning EU cybersecurity and privacy laws is difficult because the laws embody distinct regulatory philosophies – they pursue different objectives and apply different conceptual frameworks. NIS 2 is fundamentally risk based, focusing on operational resilience and incident response. The CRA is safety based, oriented towards product conformity and lifecycle security. The GDPR breach-notification rules are grounded in fundamental rights protection. The EHDS introduces sector-specific obligations for data governance.

The Digital Omnibus seeks to consolidate incident-reporting obligations across multiple EU laws – a worthy goal. It may not go far enough in standardising definitions, notably on incident severity, or reporting time frames. The degree to which consolidated incident reporting is politically feasible remains to be seen.

The better regulation process: creating, evaluating, improving, and simplifying EU laws and regulation

The EU's regulatory ambition is substantially outpacing the ability of firms and Member States to implement the laws and regulations that are being enacted; however, there does not appear to be any willingness to slow the pace of passing new laws. It will therefore be necessary to improve the quality and efficiency of the process through which laws are produced, reviewed, and enhanced.

The EU's better regulation process comprises:

- (i) *ex ante* impact assessment to ensure that legislative proposals are thought through carefully before they are submitted;
- (ii) *ex post* evaluation to periodically review whether the individual laws already in place are still relevant to the problems they were meant to address, are effective and efficient in addressing them, and are still consistent with the EU legislative *acquis*;
- (iii) flanking measures to periodically trim back bloat in the *acquis*; and
- (iv) supporting strategies and measures.

Even though the EU's better regulation process consistently ranks well in international assessments, there are opportunities for improvement in all three areas.

For the better regulation regime as a whole, one overall problem is the mounting complexity of the better regulation process over the past 20 years. This has slowed the legislative process, but the increased complexity has not necessarily produced a

corresponding gain in legislative quality. The focus on quantifiable, measurable effects tends to lead to a ‘lamppost effect’-- we look for the lost coin under the lamppost because the light is better there, even though that is not where the coin was in fact lost – better regulation measures how a law is implemented, often ignoring the more fundamental question of the degree to which the law solves the problem for which it was intended. Relatedly, the primary interest tends to be on administrative costs, rather than on the often much higher costs of operational implementation and market impacts (revenues, margins, and distributional effects).

A second overall problem is that better regulation is largely left to the Commission, even though the Commission, Parliament, and Council have agreed that better regulation is a joint responsibility.

A third overall concern is that the need to look across policy silos has grown. The silo structure of the Commission makes this difficult; also, the Commission may lack the necessary specialised expertise. Fragmentation is not solely a matter of divergence between the EU and Member State law, but also stems from overlaps and inconsistencies among different EU laws, and from implementation and enforcement differences at the Member State level.

Impact assessments are often well done, but not always; yet, only 60% of Commission proposals that go through the ordinary legislative procedure are accompanied by impact assessments. The Commission often neglects to submit impact assessments that should have been required, typically based on unconvincing claims of urgency.

Public consultation is a key building block for proper impact assessment, but consultations often fail to fully capture the views of SMEs, or even of EU independent agencies. The impact assessment is supposed to take impacts on SMEs into account, together with the overarching impact on innovation, but these parts of the assessment are typically ineffective, last-minute ‘box-ticking’ exercises.

A final issue with the impact assessment is that it corresponds to an assessment of a legislative measure as submitted by the Commission, not as enacted. Parliament and the Council are under little pressure to refrain from adding ‘feel good’ provisions whose costs and impacts are not analysed until years later, if ever.

Turning now to *ex post* evaluation, there is very little pressure to do the evaluation well, or for that matter, to do it at all. Newer laws usually include a schedule for evaluation, and these are usually adhered to; in the past, it is likely that not as many evaluations were conducted as should have been.

On the flanking measures intended to reduce legislative and regulatory bloat, the Commission's new focus on simplification and implementation is important and positive, but it is too soon to say whether it is effective. Simplification is not simple – it takes hard work, and proper analysis – merely setting a percentage goal is of limited value.

Most of the existing strategies and programmes that seek to reduce bloat, or to mitigate its consequences for the single market, are underperforming in one way or another.

- The 'one in, one out' strategy needs re-thinking – it seeks to optimise the wrong things.
- The 'Think Small First' strategy is largely aspirational rather than operational. A general problem is that SMEs are often suppliers to larger firms; consequently, exemptions meant to reduce burdens on SMEs tend to have only limited practical effect.
- Fragmentation of Member State law and regulation continues to be a burden for cross-border business. The SOLVIT network and the Single Digital Gateway (SDG) potentially represent important contributions to cross-border commerce and e-commerce, but they fall short of their potential.

Recommendations

We provide here a short synopsis of the most important recommendations developed by the Task Force.

The Digital Markets Act

Fundamental challenges with the DMA are (i) that KPIs for success are lacking, and (ii) that it is far more dependent on guidance and dialogue than expected, but these are also lacking.

- There is a need for a clear and outcome-oriented framework of indicators for contestability, fairness, and innovation, specifying the data to be collected. Independent expertise is likely to be needed.
- There is a need to standardise compliance reporting and output KPIs through a consultative process.
- A vetted-researcher mechanism modelled on Article 40 of the DSA could have merit.

The Digital Services Act

As with the DMA, firms need more guidance on DSA compliance. Also, implementation has been slow and uneven.

- The DSA implementation gap must be closed in every Member State – a DSC must be designated, sufficiently resourced, and fully empowered.
- A common set of verifiable outcome indicators for content moderation and systemic-risk mitigation is urgently needed, so that compliance can be judged on comparable evidence rather than on the platforms' self-declared figures or on the level of fines imposed.
- Additional guidance, criteria, and best practices for the independent audits required under the DSA are called for, building on existing assurance frameworks such as ISAE 3000 (Revised).

The AI Act

The need for additional guidance may be even more pressing for the AI Act than for the DMA and DSA.

- The Commission should give priority to promptly providing harmonised standards and practical, example-based guidance.
- There may well be a continuing need to clarify AI liability.

The better regulation process

Process improvements are called for in all three aspects of better regulation: (i) impact assessment, (ii) evaluation, and (iii) measures to contain or mitigate complexity.

- Reducing fragmentation requires a mix of measures that strengthen consistency in implementation and improve the practical functioning of the single market while still recognising that decentralised implementation has its place. The EU should make greater use of regulations and explicit maximum harmonisation clauses to limit divergent national interpretations; reinforce Member State implementation capacity through targeted funding, training, and technical assistance; and ensure that guidance, templates, and standardised procedures are available early enough to reduce the risk of inconsistent national approaches.
- With few exceptions, legislative proposals should be accompanied by impact assessments. Even in cases of genuine urgency, an abbreviated impact assessment should follow a few months later if feasible.

- Late in the process but prior to final enactment, an addendum to the impact assessment should be prepared to summarise the differences between the law as proposed and the law as enacted, including economic implications.
- New laws should establish a default schedule for subsequent evaluation; however, this should not preclude joint evaluation of multiple interrelated measures.
- The Commission should not be responsible for evaluating legislation *ex post*. Moving the function to, for instance, the Court of Auditors, together with assigning it sufficient staff resources, could lead to more objective and impartial evaluations.
- The *ex post* evaluation must consider whether a law is actually mitigating the problem for which it was created. Impact assessments need to do a better job of ensuring that the data required for proper subsequent evaluation are collected.
- The Commission should be making greater use of the regulatory fitness and performance programme, REFIT, to simplify existing laws so as to reduce needless regulatory complexity.
- The omnibus process could be valuable, but its effectiveness has been limited to date by process deficiencies in how it has been implemented. Simplification is by no means simple. Proper consultation and analysis are needed. Where changes with complex implications are put forward, the Commission must conduct a proper impact assessment. Purported urgency is not an excuse.
- Several programmes that aim at simplification, burden reduction, and mitigation of fragmentation need serious revision.
 - The one in, one out programme is genuinely promising, but it needs serious rethinking if it is to deliver on its promise.
 - The SOLVIT network should be strengthened and modernised so that it becomes a genuinely useful tool for cross-border merchants rather than a little-known mechanism used mainly by individuals.
 - The Single Digital Gateway (SDG) should evolve from a document repository into a genuinely usable compliance tool for cross-border merchants. To achieve this, more and better online tools are needed; SDG content must become easily discoverable through search engines; and merchants should encounter clear summaries as well as alerts for regulatory changes rather than raw documents alone

1. INTRODUCTION

Objectives

CEPS convened a Task Force of knowledgeable industry stakeholders, academic experts, and NGO representatives under the Chatham House Rule, to think through what is needed to reform and reinvigorate the EU digital *acquis*. The Task Force also considered the process through which EU laws and regulations are designed, implemented, enforced, reviewed, and enhanced over time, with a specific focus on the digital world.

The call for reform is timely and widely considered to be necessary in light of the exploding complexity of EU law and the consequent need for simplification, as highlighted in Draghi (2024b), as well as for boosting EU productivity and competitiveness overall. It further reflects the necessity of strengthening the EU's open strategic autonomy, given the increasingly tense geopolitical environment and the deterioration of the transatlantic relationship.

As we are still early in the 2024–29 mandate, this is a suitable time to provide concrete reflections and advice to policymakers at the EU and Member State levels.

Background

The aggregate complexity of EU law for the digital world has become enormous, and the pace with which new laws are enacted shows no signs of slowing down. At the same time, the need for various forms of regulation is unquestionably growing.

EU laws and regulations dealing with the digital world have greatly expanded in many dimensions in recent years. In just the past dozen years, the number of laws related to digitalisation has more than quadrupled, from roughly 20 to 88. Moreover, the average length of EU laws has doubled over the past 20 years. Relatedly, the interactions among the various digital laws appear not only to be mounting, but also to have reached the point where even the best experts struggle to identify them all.

In the most recent legislative term, the Digital Markets Act (DMA), Digital Services Act (DSA), Data Act, Artificial Intelligence Act, Data Governance Act, and the Cyber Resilience Act (CRA) were passed, in addition to broad sectoral measures such as the European Health Data Space (EHDS). These were on top of complex laws already in place, including the General Data Protection Regulation (GDPR) and the European Electronic Communications Code. Some of these laws do provide opportunities for EU firms – but all of them impose regulatory burden.

At a time when many experts have called for a pause in enacting new EU law to enable businesses and the Member States to catch up, and with the Draghi (2024b) and Letta (2024) reports both calling for regulatory simplification, the number of new laws proposed by the European Commission seems to still be moving forward at a breakneck pace.

EU businesses, especially SMEs, pay a substantial price for this complexity (Marcus et al., 2025). How are they to manage it? For the EU public, the current state of play is barely comprehensible.

At the same time, the need for EU rules is clear enough and expanding for many reasons. The centrality of digital goods and services in the everyday lives of Europeans has steadily increased. The concentration of de facto power in the hands of a small number of firms headquartered outside the EU raises multiple concerns. The risk of malicious disinformation and election manipulation has grown markedly, and the ever more fractious transatlantic relationship does not help. America's reliability as a technology supplier could be subject to sudden, arbitrary shocks, and there is also a risk of supply chain disruption involving China. The threat of cyberattacks from commercially motivated hackers and from government-sponsored actors has compounded.

Both businesses and society need protection from these numerous threats.

The importance of improving the effectiveness, efficiency, and quality of EU legislation, and of making it less burdensome for businesses large and small, is consequently manifest. This necessarily relates not only to the substance of existing laws but also to the process through which they are created, evaluated, and improved over time.

None of this is easy – simplification is not simple. Striking the right balance between, on the one hand, protecting EU firms and the public, and avoiding needless regulatory burden on the other, has proven to be challenging.

Methodology

Many of the issues identified by the Task Force are not altogether new, especially in the process-oriented portions of the report. We drew on the literature, including our own work, to supplement Task Force deliberations. We also drew on previous findings to augment this report.

This report provides key observations and recommendations, reflecting those discussions, together with the background to frame them. In some instances, we have added our own observations either to round out the discussion or else to reflect events that took place after the last Task Force meeting – the landscape is rapidly evolving.

The report can be viewed as a *curated distillation* of a more complex discussion. We have attempted to organise and prioritise what was said, while conveying the degree of support within the group that the various ideas seemed to enjoy.

Subsequent regulatory proposals

The Commission is continuing to make important legislative proposals. Open strategic autonomy is a prominent ongoing theme, as exemplified by the Chips Act 2.0 (2026/0139 (COD)). The Commission has also announced a pending Cloud and AI Development Act, and has issued additional strategy documents. In this report, we do not cover these legislative proposals because they were not discussed with the Task Force participants. Other areas of continued focus are child protection and the Digital Fairness Act.

Structure of the remainder of this report

Following this introduction, Section 2 looks at the explosive growth in the number of digital laws. Sections 3 through 7 then deal with major clusters of digital laws: Section 3 with digital sovereignty; Section 4 with competition and the level playing field; Section 5 with fundamental freedoms; Section 6 with AI; and Section 7 with privacy, data sharing, and cybersecurity. Section 8 considers not the individual laws, but rather the process through which the EU creates, reviews, and improves its legislative *acquis*.

Key findings for Sections 2 through 8 appear at the very beginning of each of these sections.

Recommendations are numbered and appear at the point in the narrative where they are first introduced in each of those sections. The list of recommendations (following the contents list at the beginning of the report) presents the recommendations in numerical order, with a page number to enable the reader to identify the basis and substantiation for each one.

Appendix A provides a list of Task Force participants, and Appendix B the principles and guidelines of the Task Force.

2. EXPLOSIVE GROWTH IN THE NUMBER AND COMPLEXITY OF EU ‘DIGITAL’ LAWS

Key findings

Simplification has become a major focus of the current five-year EU legislative mandate, in line with the Draghi report. This emphasis is appropriate.

The number of EU laws for the digital world, and the rate of growth in complexity, is daunting.

- From 2012 to 2024, the number of digital laws rose from 20 to 88.
- The average length of all EU laws has roughly doubled over the past 20 years.
- Each law consists of multiple provisions, any one of which might conflict with provisions in other laws. But even if we look at the much simpler question of how many laws might have an interaction with some other law (ignoring the provisions within each law), then according to basic mathematics, the number of two-way interactions among 88 laws is 3,828.

No human expert could hope to identify all of the potential conflicts and inconsistencies without considerable automated support. Automated tools have not yet demonstrated their ability to deal with this complexity, but the day may be coming.

The Draghi report (2024b) emphasised the need to simplify and re-focus EU law. Simplification has become a central part of the current von der Leyen II mandate from 2024 to 2029. A quick glance at the few statistics demonstrates that this focus is not misplaced.

There is now a daunting volume of EU law in the digital space (see Table 1) (Zenner, Marcus, & Sekut, 2025). Not only is the current volume of EU digital law intimidating, but also the pace at which new laws appear seems to be accelerating on something that approximates an exponential growth curve (see Figure 1), based on the data provided by Zenner, Marcus, & Sekut (2024). As recently as 2012, only 20 digital laws had been enacted; as of summer 2024, it was something like 88 – a quadrupling in just over a decade. Subsequent CEPS editions of the dataset demonstrate continuing growth in the number of EU digital laws in force.

Aside from the number of laws, the length of all EU laws has roughly doubled over the past 20 years (Sekut & Marcus, 2024).

To say that the number and length of laws have increased dramatically does not tell us exactly what the impact is on firms, individuals, or Member States that have to implement the laws; however, it is fair to say that if the number and length are going up, it is unlikely that the complexity of the task is going down.

The number of unintended conflicts or inconsistencies among these laws is far greater than the number of laws alone would suggest. Each law consists of multiple provisions, any one of which might conflict with provisions in other laws. But even if we look at the much simpler question of how many laws might have an interaction with some other law (ignoring the provisions within each law), then according to the well-known formula for the binomial coefficient for unordered pairs, the number of two-way interactions among 88 laws is 3,828.

Clearly, no human expert would be able to identify all of the risk areas without considerable automated support. Automated tools have not yet demonstrated their ability to deal with this complexity, but the day may be coming.

Table 1. EU digital-sector rules at a glance

Overview of EU Legislation in the Digital Sector

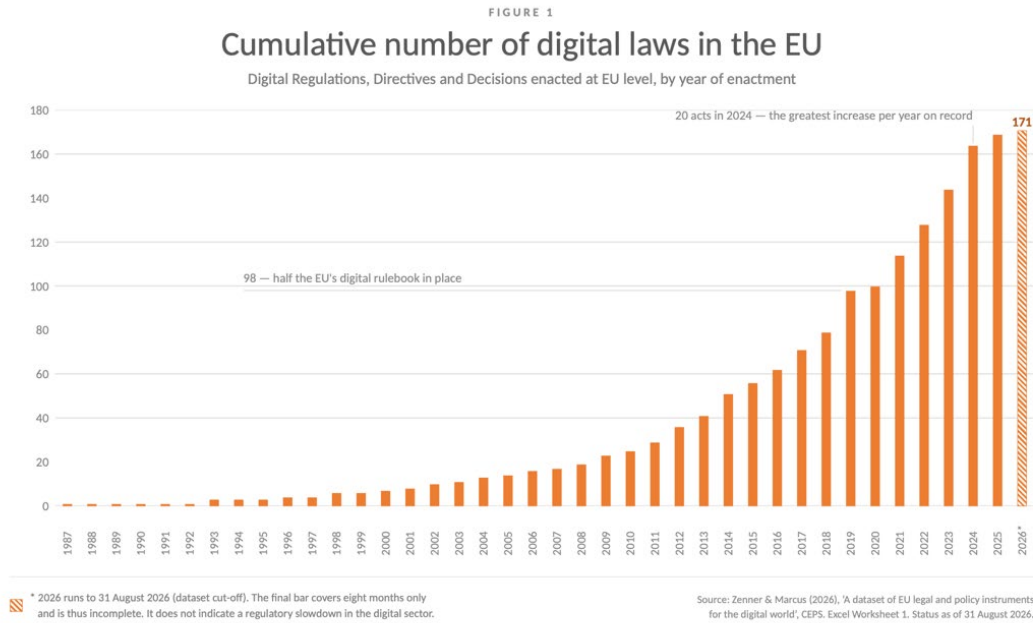
Research, Innovation & Emerging Technologies	Industrial Policy & Strategic Autonomy	Connectivity & Digital Infrastructure	Competition & Market Access	Product Safety, Compliance & Standards	Intellectual Property & Digital Creativity	Data Governance, Privacy & Digital Identity	Cybersecurity & Digital Resilience	Platforms, Online Services & Media	Digital Consumer Rights & E-Commerce	Digital Justice, Security & Rights	Sectoral Digital Transformation
European Research Infrastructure Consortium (ERIC) (EC) No 723/2009	European Venture Capital Funds (EUVCs) (EU) No 345/2013	Radio Spectrum Framework 87/372/EEC 436/2006/EC 243/2013/EU (EU) 2019/3389	Implementation of Competition Rules in Art 101 & 102 TFEU (EC) No 1/2003	New Legislative Framework 67/737/EEC (EC) No 765/2008 No 186/2008/EC (EU) 2019/1009	Content Access Framework 55/84/EEC 96/94/EC (EU) 2015/789	ePrivacy Directive 2002/58/EC	Cybersecurity Act (EU) 2019/881	e-Commerce Directive 2006/12/EC	Consumer Contract & Fairness Framework 19/2011/EU, 2011/83/EU	CSAM Directive 2011/93/EU	Common System of VAT 2006/115/EC
Digital Europe Programme (EU) 2021/2404	Screening of Foreign Direct Investments (FDI) (EU) 2019/452	Open Internet Regulation (Net Neutrality) (EU) 2015/2120	EC Merger Regulation (EC) No 139/2004	Electrical & Electronic Equipment Compliance 2011/65/EU, 2011/76/EU, 2014/76/EU, 2014/78/EU	Databases Directive 96/76/EC	INSPIRE Directive (Directive8459) 2007/2/EC	European Cybersecurity Competence Centre (ECC3) (EU) 2021/887	Audio-Visual Media Services Directive (AVMSD) 2018/1875	ADR Directive 2013/11/EU	Cybercrime Directive 2013/40/EU	Digital Payments 2008/118/EC (EU) 2017/748 (EU) 2015/2366
Horizon Europe Framework (EU) 2021/795, (EU) 2019/746, (EU) 2021/764	Energy & Grid Capacity Framework (EU) 2019/946, (EU) 2022/869	Web Accessibility Directive (EU) 2016/2102	Services Directive 2006/123/EC	European Standardisation Regulation (EU) No 1025/2012	Information Society Directive 2011/79/EC	European Statistics Regulation (EC) No 215/2009	NIS 2 / CBR Framework (EU) 2022/2555, (EU) 2022/7957	Platform To Business Regulation (PTB) (EU) 2019/1510	Portability Regulation (EU) 2017/1218	Law Enforcement Directive (EU) 2016/680	Intelligent Transport 2010/40/EU (EU) 2017/748 (EU) 2019/1020, (EU) 2020/7496
European Defence Fund (EDF) (EU) 2021/687	Recovery and Resilience Facility (RRF) (EU) 2021/241	BEREC Regulation (EU) 2014/1875	Union Customs Code (EU) No 952/2013	Radio Equipment Directive (RED) 2014/79/EA	IP Enforcement Framework (IPRED) 2004/48/EC (EU) No 449/2013	atLAS Regulation (EU) 2021/2014	Cybersecurity Regulation (EU) 2022/2841	Terrorist Content Online (TCO) (EU) 2021/784	Consumer Protection Cooperation Regulation (CPC) (EU) 2017/2384	PAR Directive 2014/682	Administrative Cooperation in the Field of Taxation (DAC) 2011/16/EU
European Institute of Innovation and Technology (EIT) (EU) 2012/1819	InvestEU Programme (EU) 2021/233	European Electronic Communications Code (EECC) (EU) 2018/1872	Public Procurement Law 2014/23/EU, 2014/24/EU, 2014/25/EU, 2014/74/EU	Energy Labelling Regulation (EU) 2017/1369	Software Directive 2009/24/EC	General Data Protection Regulation (GDPR) (EU) 2016/679	Cyber Resilience Act (CRA) (EU) 2024/2847	Digital Markets Act (DMA) (EU) 2023/2863	Geo-Blocking Regulation (EU) 2018/302	Europert Regulation (EU) 2024/794	Digital Health Products (EU) 2017/746, (EU) 2017/786
Joint Undertaking for High Performance Computing (EuroHPC) (EU) 2022/1173	Dual-Use Regulation (EU) 2017/2453	Ja-Taxi Level Directive (EU) 2018/1031	General Block Exemption Regulation (GBER) (EU) No 651/2014	European Accessibility Act (EU) 2019/1862	Orphan Works Directive 2012/28/EU	EU Data Protection Regulation (EU) 2018/1725	Cyber Solidarity Act (EU) 2023/106	Digital Services Act (DSA) (EU) 2022/2865	Single Digital Gateway (EU) 2016/1033	European Public Prosecutor's Office (EPPO) (EU) 2017/1939	General Safety Regulation for Vehicles (EU) 2019/2144
Chips & SPS Joint Undertaking under Horizon Europe (EU) 2022/2085	Digital Decade Policy Programme (DDPP) (EU) 2022/2444	Union Space Programme Regulation (EU) 2014/536	Technical Regulations Information System (TRIS) (EU) 2013/1535	General Product Safety Regulation (GPSR) (EU) 2013/1888	Utility Patent & Compulsory Licensing (EU) 125/2002, (EU) 1286/2012, (EU) 2021/2445	Free Flow of Non-Personal Data (EU) 2018/1807	Information Security Regulation 2022/20840/00	Political Advertising Regulation (PAR) (EU) 2024/1966	Digital Content Directive (EU) 2019/770	ex-LISA Regulation (EU) 2018/1726	Prior Regime Distributed Ledger Technology (DLT) (EU) 2022/2618
European Innovation Act (EU) 2024/180	Chips Act (EU) 2023/1781	Connecting Europe Facility (CEF) (EU) 2013/1551	Company Law Directive (EU) 2017/1132	Machinery Regulation (EU) 2013/2320	Collective Rights Management 2014/94/EU	Open Data Directive (ODD) (EU) 2019/1054	European Media Freedom Act (EMFA) (EU) 2024/1983	European Media Freedom Act (EMFA) (EU) 2024/1983	Sale of Goods Directive (EU) 2017/751	Europert Regulation (EU) 2018/1737	Digital Operational Resilience Act (DORA) (EU) 2022/2554
Quantum Act (EU) 2024/180	Strategic Technologies for Europe Platform (STEP) (EU) 2024/795	Roaming Regulation (EU) 2012/612	Aircraft Block Exemption (EU) 2022/7730, (EU) 2013/1066, (EU) 2016/1067	Batteries Regulation (EU) 2023/1842	Trade Mark Framework (EU) 2017/1369, (EU) 2017/1001	Data Governance Act (DGA) (EU) 2023/3668		Platform Work Directive (PWD) (EU) 2024/2811	Representative Actions Directive (RAD) (EU) 2020/1828	Combating Fraud and Counterfeiting of Non-Cash Means of Payment (EU) 2018/711	Crypto Assets Regulation (CAR) (EU) 2023/1113
European Research Area Act (ERA) (EU) 2024/180	Critical Raw Materials Act (CRM) (EU) 2024/1252	Union Secure Connectivity Programme (USCP) (EU) 2019/1488	Single Window Environment for Customs Regulation (SWC) (EU) 2022/7395	AI Act (EU) 2024/1689	Trade Secrets Directive (EU) 2016/949	Data Act (EU) 2018/1804		Consumer Credit Directive II (EU) 2018/912	Interoperability Regulations (EU) 2018/912	European Single Access Point (ESAP) (EU) 2017/2859	European Single Access Point (ESAP) (EU) 2017/2859
	Net Data Industry Act (NDIA) (EU) 2024/1795	Interoperable Europe Act (EU) 2023/905	Foreign Subsidies Regulation (FSR) (EU) 2022/2540	Eco-Design for Sustainable Products Regulation (ESPR) (EU) 2024/1781	Copyright Directive (EU) 2019/790	Data Collection for Short-Term Rental (EU) 2024/1609		Right to Repair Directive (EU) 2024/1789	Law Enforcement Access to Financial Information Directive (EU) 2017/1313	Anti-Money Laundering Package (EU) 2023/1113, (EU) 2024/1620, (EU) 2024/1624, (EU) 2024/1640	European Health Data Space (EHDS) (EU) 2022/2927
	Internal Market Emergency and Resilience Act (IMER) (EU) 2024/2747	Digital Infrastructure Act (DIA) (EU) 2019/1309	3RD regime (EU) 2020/2070(CO)00	Product Liability Directive (PLD) (EU) 2019/1783	Design Protection Framework (EU) 2019/2383	Harmonisation of GDPR Enforcement Procedures (EU) 2022/2520	Digital Fairness Act (EU) 2024/2847			e-CODES Regulation (EU) 2022/2650	European Health Data Space (EHDS) (EU) 2022/2927
	European Competitiveness Fund 2021/771(EPF)	EU Space Act 2021/013(CO)00	Single Market Barriers Prevention Act (SQM) (EU) 2023/2027	Toy Regulation (EU) 2015/2369		European Business Warrant 2021/0138(CO)00			E-evidence Framework (EU) 2013/1441, (EU) 2013/1444	EU Talent Pool (EU) 2022/1544	
	Industrial Accelerator Act (IAA) 2024/098(CO)00	Digital Networks Act (DNA) 2024/061(CO)00		European Product Act (EPA) (EU) 2024/180		Harmonised EU Data Requirement Framework (2027)			Digitalisation of Cross-Border Judicial Cooperation (EU) 2023/2844	Financial Data Access Regulation (FDA) 2023/1620(CO)00	
	Cloud and AI Development Act (CADA) 2024/0118(CO)00	EU Critical Communication System (ECCS) (EU) 2024/180							PRISM II Regulation (EU) 2024/2847	Digital Euro 2023/281(CO)00	
									Child Sexual Abuse Regulation (CSAR) 2022/0116(CO)00	Rail Ticketing & Multimodal Booking Package 2024/0113(CO)00, 2022/0113(CO)00	
									EU Digital Travel Application 2024/0110(CO)00	Skills Portability Initiative (EU) 2024/180	
									Digitalisation of the Return Process (EU) 2024/180	Quality Jobs Act (EU) 2024/180	

-  **Applicable law**
-  **Updated law**
-  **In Process**
-  **Planned initiative**

Legally binding act after being published in the Official Journal of the European Union.
The applicable law or parts of it are being updated by the co-legislators.
Proposal by the European Commission has entered the legislative process of the EU.
Officially pronounced in the Commission's work programmes, addressed in the State of the European Union speech or stated by a Commissioner.

Source: Zenner, Marcus, & Sekut (2025).

Figure 1. Cumulative number of EU laws dealing mainly with digitalisation



Source: Marcus & Rossi (2024) based on Zenner, Marcus, & Sekut (2024).

A recent Bruegel study (Bucher & Golberg, 2026a) found not only a dramatic increase in the number of new laws, but also a huge number of delegated and implementing acts adopted under the ordinary legislative procedure (see Table 2 and Table 3).

Table 2. Commission proposals and adopted acts under the ordinary legislative procedure (2014–24)

Commission term	Proposals: basic acts	Proposals: amended acts	Withdrawals	Net proposals	Adopted basic acts	Adopted amended acts	Total adopted	Exp/R	Net balance, adopted acts
2014-2019 (Juncker)	243	165	62	346	242	161	403	230	173
2019-2024 (von der Leyen)	252	210	23	439	244	191	435	239	196

Source: Bucher & Golberg (2026a) based on EUR-Lex.

Note: Exp/R = expired and repealed acts; balance adopted = total adopted legislation less expired acts and repeals.

Table 3. Delegated and implementing acts under the ordinary legislative procedure (2014–24)

Commission term	Delegated acts basic	Amended delegated acts	Total	Delegated acts exp/R	Balance delegated acts	Implementing acts basic	Amended implementing acts	Total	Exp/R	Balance adopted
2014-2019	309	312	621	62	559	2728	1778	4506	1032	3474
2019-2024	350	584	934	222	712	3058	2073	5131	2215	2916

Source: Bucher & Golberg (2026a) based on EUR-Lex.

Note: Exp/R = expired and repealed acts; balance adopted = total adopted implementing acts less expired acts and repeals.

3. DIGITAL SOVEREIGNTY, OPEN STRATEGIC AUTONOMY, AND INDUSTRIAL POLICY

Key findings

Reducing the EU's strategic risk in light of growing geopolitical threats and continual tensions in the transatlantic relationship is widely understood to require attention. The change in the transatlantic relationship has been a key driver – the US is the EU's main technology supplier, but it has evolved from a reliable ally to at best a much less predictable actor.

The EU's strategic autonomy goals have not always been clearly articulated – the term *open strategic autonomy* embeds a tension of objectives. The EU has always been strongly committed to global openness, in terms of global value chains and international institutions; however, there are questions as to whether these goals can be fully maintained in the face of worsening global tensions. Global and local value chains are threatened by kinetic war, naval blockades, natural and man-made disasters, high and arbitrary tariffs imposed abruptly for any reason or for no reason, and export controls. International organisations are under great threat and have little or no ability to enforce their decisions. The tension is often expressed as a need to be as open as we can be, while being as closed as we must be.

Nobody is seriously promoting full EU autarky – it is not possible for the EU alone to produce every technology good and service that it needs, just as it is not possible for any region in the world to be entirely self-reliant. But this implies a need for the EU to choose our priorities carefully. Risk assessment is called for, following the classic model of evaluating (i) how likely a risk is to eventuate, (ii) what is the cost if it does, and (iii) what would it cost to guard against the risk. To successfully implement this, we need an in-depth understanding of our dependencies.

A mix of mitigation measures are likely to be required, aligned with EU values, for critical goods and services: (i) increasing the ability of the EU to self-supply or to provide fall-back solutions for vital sectors; (ii) enhancing resilience by building more diverse and robust international supply chains; (iii) aiming to achieve 'strategic indispensability', where the EU holds leverage in specific niches; and (iv) collaborating more closely with like-minded third countries and trustworthy technology partners. Flanking measures are likely needed to protect intellectual property, and to retain and expand talent and capital in the EU.

Reducing the EU's strategic risk in light of growing geopolitical threats, including the progressive deterioration of the transatlantic relationship, requires urgent attention.

The recognition of these needs has risen to policy prominence since 2024 under the heading of *open strategic autonomy* or *digital sovereignty*, but it has not always been clear what policymakers mean by these terms. For the purposes of this report, we can think of these terms as denoting the ability of the EU to establish and implement its own goals for the digital world, without having them dictated by third countries such as China or the US.

The term *open strategic autonomy* embeds a tension of objectives. The EU has always been strongly committed to global openness, in terms of global value chains and international institutions; however, these goals cannot be fully maintained in the face of growing global tensions. Global and local value chains are threatened by kinetic war, naval blockades, natural and man-made disasters, high and arbitrary tariffs imposed abruptly for any reason or for no reason, and export controls. International organisations are under great threat, and have little or no ability to enforce their decisions.

In this ever more tense world, the EU has to strategically defend its interests. It must increase resilience and supply chain diversity while mitigating threats to value chains, protecting intellectual property, and taking steps where feasible and where consistent with EU values to retain and expand talent and capital in the EU.

The US is the EU's main technology supplier, but it has to be viewed in a different light from that of the recent past as it evolves from a reliable ally to at best a much less predictable actor. Repeated US statements regarding Greenland – including explicit threats of military action to seize the territory – have raised concerns among European policymakers about the reliability of US security commitments. Recent US actions in the digital sphere have added to these concerns. The abrupt prohibition on the sale of Anthropic and OpenAI products to foreign users – imposed without prior consultation and affecting allies as well as adversaries – has been interpreted by many European policymakers as further evidence of a progressively more unilateral US approach to security-related technologies. These developments underscore the need for Europe to strengthen its own resilience.

This need has been recognised by the EU institutions and is most recently demonstrated by a series of strategies and laws proposed by the Commission as part of a new European Technological Sovereignty Package on 3 June 2026, notably the Chips Act 2.0 (2026/0139 (COD)) and the Cloud and AI Development Act (announced on 3 June 2026 but not yet formally submitted).

It is widely acknowledged that it is not possible for the EU alone to produce every technology good and service that it needs, just as it is not possible for any region in the world to be entirely self-reliant. For some critical goods and services, the EU will be able to increase its ability to self-supply; for others, it will be necessary to try to build more diverse and robust supply chains. Often, a mix of the two approaches will be called for. It might be that a third approach is also needed: if full sovereignty is not achievable, it might perhaps be better to aim for ‘strategic indispensability’ where the EU holds leverage in specific niches. There is also scope for increased collaboration with like-minded third countries, and with trustworthy technology partners.

All of this implies a need for the EU to choose our priorities carefully. This in turn implies the need for risk assessment. In general, dealing with risk entails evaluating (i) how likely a risk is to eventuate, (ii) what is the cost if it does, and (iii) what would it cost to guard against the risk.

In order to assess risks, it would be essential to understand our dependencies in depth. Despite efforts on the part of Directorate-General (DG) GROW in recent years, Task Force participants were not convinced that we understand our dependencies adequately.

Several additional aspects of strategic autonomy were considered, but without reaching conclusions. As a concrete case study of how to implement open strategic autonomy, the Task Force considered the ongoing discussion of a possible *Eurostack*, an EU-based technology stack with no dependency on US or Chinese technology. Does the EU have the funding, time, and technology to catch up with its global rivals across the board? If not, what mix of the three strategies noted above is most appropriate in the near to medium term?

The Task Force also considered the huge volume of EU digital regulation already in place, with more coming (see Section 2). Does it contribute to sovereignty, e.g. via the ‘Brussels effect’, or does it function more as an impediment to EU productivity and competitiveness?

Finally, we reflected briefly on the degree to which steps taken to foster digital sovereignty inadvertently increase fragmentation of internet core functions.

4. COMPETITION AND THE LEVEL PLAYING FIELD: THE DIGITAL MARKETS ACT

Key findings

The DMA has moved rapidly from gatekeeper designation to active enforcement, with the first specification and non-compliance decisions now taken. But it remains too early to judge its effectiveness with confidence, and the criteria against which success will be assessed have not been defined in advance.

Because the DMA works through conduct obligations rather than fines, the central question is whether gatekeepers are genuinely changing their behaviour. The evidence heard was mixed and sharply contested, ranging from documented governance change to allegations of systematic or malicious non-compliance, which underlines the absence of agreed indicators.

The regime has proved far more dependent on Commission discretion and dialogue than its drafters anticipated. Gatekeepers and business users alike called for greater clarity, standardised key performance indicators (KPIs) for compliance, fuller use of specification decisions, and better-structured multilateral dialogue. Some, however, warned that dialogue has limits and must ultimately be backed by enforcement.

The DMA is not discriminatory in design in the sense that its legal provisions do not explicitly discriminate. Yet, the concentration of designated gatekeepers among US firms, and its occasional invocation as a form of digital sovereignty, have fed a powerful discriminatory-effect narrative and transatlantic trade tensions that must be managed if the regime is to endure.

Rigorous independent evaluation will require access to data that currently reside almost entirely with the gatekeepers. A bounded data-access route for vetted researchers, modelled on the DSA, and a more coherent European architecture for enforcement both merit serious consideration.

The Digital Markets Act (Regulation (EU) 2022/1925) represents a deliberate shift in EU competition policy from *ex post* enforcement, case by case and after the fact, towards an *ex ante* regime of clear, self-executing obligations imposed on a defined set of large platforms designated as gatekeepers of core platform services (Colomo, 2025; Crémer, 2023; Simone & Laudando, 2025).

The intellectual origins of this shift lie in the recognition that traditional competition law, with its lengthy investigations and case-specific theories of harm, struggled to keep pace with the speed and network effects of digital markets. Certain structural features of those markets (tipping, self-preferencing, and the accumulation and combination of data) called for rules rather than adjudication (Chirita, 2022; Podszun, 2021; Crémer et al., 2023). Commission officials involved in enforcement confirmed to the Task Force that the DMA was created precisely because competition policy alone was judged insufficient to address the concentration and entrenched practices that emerged as digital markets matured from open, high-opportunity spaces into markets dominated by a few players. The officials confirmed that, in the Commission's view, this founding rationale remains valid two years on.

The DMA's twin objectives are contestability (keeping markets open to challengers) and fairness, ensuring an equitable distribution of value between gatekeepers and their business users (Pošćić, 2024; Lee, 2024).

The first wave of designations, and their partial testing before the General Court in the ByteDance proceedings, has established the basic contours of who falls within scope and on what basis (Bostoen & Monti, 2025; Humpe et al., 2024; Leslie et al., 2025).

With the core obligations now in force, and the first specification and non-compliance decisions taken against Apple, Meta, and Alphabet, the centre of gravity has shifted from the question of designation to the harder questions the Task Force considered most pressing: whether the regime is achieving its aims, and how anyone would be able to tell.

4.1. IS IT TOO EARLY TO JUDGE EFFECTIVENESS, AND WHAT WOULD SUCCESS LOOK LIKE?

A recurring theme of the Task Force's discussions, and of a previous dedicated stakeholder roundtable on the DMA, was that it is genuinely too early to reach firm conclusions about the regime's effects, and that this difficulty is not merely a function of the limited time the obligations have been in force. The Commission's evaluation, required under Article 53 DMA, was scheduled for 2026 – barely two years after the obligations first bit.

Several participants close to the process observed that the phased entry into force of more than 20 obligations across different categories of core platform services makes like-for-like assessment inherently hard. The arrival of generative AI products after the DMA was designed further muddies any attempt to attribute market changes to the regulation (Botta, 2026; Simone & Laudando, 2025). The two statutory objectives, contestability and fairness, are considerably easier to state than to measure; any observed change reflects a dense web of confounding factors that cannot readily be disentangled from the effect

of the law itself. This concern was sharpened by a striking disagreement about the evidence base.

A consumer survey presented to the roundtable reported that a majority of Europeans felt they had to search longer for relevant information than before the DMA. It further reported that a substantial minority perceived less useful personalisation, and that many said they would pay a modest sum to restore features they associated with the pre-DMA experience. The presenter was careful to describe this as a temporal association rather than proof of causation.

Others were more sceptical still of the state of knowledge. An economist participant argued that the DMA lacks any effects-based mechanism for measuring harm or benefit, so that gatekeepers can always be told they are not yet compliant while no one can specify the counterfactual against which success would be judged – a gap several speakers warned would return to haunt the Article 53 review. Commentators responding to the review had made the same point in print, arguing that clear and objective metrics, specified in advance, are indispensable if the regime is to be assessed on evidence rather than by advocacy (International Center for Law and Economics, 2025; Digital Competition, 2025).

The Commission's own review reported that the DMA had introduced or increased competition and enabled new market entry (European Commission, 2026d; Tech Policy Press, 2026b). Participants, however, noted that its consultation drew responses skewed towards business users and SMEs, that only the seven designated gatekeepers responded from that side, that around a quarter of respondents disclosed a commercial relationship with a gatekeeper, and that the exercise was largely impressionistic – a survey of opinion rather than a source of new economic data. Several were therefore sceptical of an evaluation in which the Commission, in effect, grades its own homework.

The Task Force's conclusion was not that the review is without value – it is required and is a valuable discipline – but that a credible assessment should rest on a framework of indicators defined in advance and, ideally, applied by a body independent of the enforcer. One participant suggested that the most useful thing the Commission could do now is prepare a rigorous evaluation framework for application in two to three years, rather than repeat a premature exercise.

Recommendation 1. The Commission should, without waiting for the next review cycle, publish a clear and outcome-oriented framework of indicators for contestability, fairness and innovation, specifying the data to be collected. It should commission at least part of the resulting assessment from a body independent of its own enforcement function.

4.2. ARE GATEKEEPERS CHANGING THEIR BEHAVIOUR, AND IS COMPLIANCE GENUINE?

Because the DMA works through conduct obligations rather than fines, the central empirical question is whether gatekeepers are actually changing their behaviour, and whether those changes are genuine. The evidence heard by the Task Force was mixed and sharply contested.

On one side, an independent benchmarking of the published compliance and audit reports of gatekeepers found real behavioural change, dedicated DMA governance structures, internal audit functions, and revised consent and policy mechanisms that represent a clear break from the pre-DMA era. Yet it cautioned that the depth of reporting varies enormously between firms, that audits are point-in-time snapshots, and that cross-gatekeeper comparability is poor (KPMG, 2025). A gatekeeper representative described devoting very substantial engineering and executive resources to compliance, a six-month consultation with roughly a thousand developers, and weekly internal compliance reviews, and reported relatively positive market feedback on changes such as the browser-choice screen.

On the other side, a consumer-organisation representative reported having filed numerous submissions alleging systematic, incomplete, or in some cases malicious non-compliance, and argued that it is premature to draw any conclusion about benefits while so much non-compliance persists. The same speaker welcomed genuine gains, such as the iOS browser-choice screen, but attributed them to Commission pressure rather than to voluntary gatekeeper action.

An industry economist pushed back on the very framing of malicious non-compliance, arguing that the obligations are genuinely difficult to implement, that interoperability and openness are not a free lunch and involve real trade-offs with privacy and security, and that pressing for more aggressive enforcement now could make outcomes worse rather than better.

These are not easily reconciled positions, and the Task Force did not attempt to adjudicate between them; however, the disagreement itself reinforces the central point that,

without agreed indicators of behavioural change, the debate cannot move beyond competing anecdotes (Zhybak, 2024; Hornkohl, 2024).

4.3. ENFORCEMENT CLARITY, COMPLIANCE KPIS, AND THE LIMITS OF DIALOGUE

A closely related cluster of concerns involved predictability and the quality of the compliance relationship.

A recurring complaint from the gatekeeper side was that the DMA had been presented as a set of clear dos and don'ts but had proved, in application, to require far more interpretation and dialogue than expected. This leaves a great deal of discretion with the Commission and considerable uncertainty for the regulated firms and the developers who depend on them.

An in-depth study of enforcement practice presented to the Task Force, based on interviews with more than 20 stakeholders, described enforcement as resting heavily on informal bilateral interaction between the Commission and individual gatekeepers. It observed that business users were engaged less intensively and often given no feedback on the outcome of their input. It also identified an internal culture difference between the more adversarial competition-enforcement tradition and the more regulatory approach of the Commission's digital policy services, and an initial reluctance to signal what compliance solutions would be acceptable even though the burden of proposing them rests on the gatekeepers.

Business users, for their part, reported that gatekeepers' compliance reports remain weak on substantive indicators, amounting in places to box-ticking, and that they lack independent verification. From this diagnosis flowed a set of concrete proposals that the Task Force considered constructive:

- standardised process and output indicators, for example the actual uptake of interoperability or data-portability features, which would allow comparison across gatekeepers and over time;
- a strengthened compliance officer function that engages external stakeholders and gives an independent, personally accountable opinion on the effectiveness of compliance measures; and
- more and better-structured multilateral dialogue between the Commission, gatekeepers, and business users, including technical and engineering participants rather than lawyers alone, to reduce the information asymmetry that currently favours the gatekeepers (Zhybak, 2024; Hacker et al., 2023).

At the same time, a consumer representative cautioned that dialogue has limits, and that where it has plainly failed to produce compliance, the Commission must be willing to

move to substantial fines and periodic penalty payments. Fines are not the objective, but they remain the ultimate means of securing the conduct changes that are sought.

Recommendation 2. The Commission should work with gatekeepers and business users to standardise compliance reporting around agreed key performance indicators for process and output that capture the actual uptake of new openness and interoperability. It should make fuller use of the specification-decision procedure to give timely, example-based guidance on acceptable compliance and should strengthen the role of the independent compliance officer.

4.4. NON-DISCRIMINATION IN DESIGN, DISCRIMINATORY IN EFFECT?

The DMA imposes its obligations by reference to objective, quantitative thresholds and applies them equally to any undertaking that meets them, irrespective of nationality. In that formal sense, it is not discriminatory, and the legal literature broadly supports this characterisation (Simone & Laudando, 2025; Lee, 2024). This point was made forcefully at the Task Force by a researcher who observed that the principal beneficiaries of DMA-mandated openness so far are themselves American companies, and that the operative legal criterion is size, not nationality.

Yet because six of the seven designated gatekeepers are US undertakings, the regime is widely perceived abroad as having a discriminatory effect, and that perception has hardened as the transatlantic relationship has deteriorated (Istituto Affari Internazionali, 2026; German Marshall Fund of the United States, 2025). US commentary has gone considerably further, characterising the DMA as a form of discriminatory industrial protectionism, questioning its compatibility with international trade commitments, and linking it to threats of trade retaliation (Center for Strategic and International Studies, 2026a; Center for Strategic and International Studies, 2026b). Related work situates the DMA within a broader contest over the international reach of EU digital rules (Ma, 2026; Koenig, 2025).

A further complication, raised by more than one participant, is that the DMA has at times been invoked as an example of digital sovereignty, with investigations relaunched under sovereignty rhetoric quite distinct from the law's contestability-and-fairness rationale.

A representative of one large platform questioned why an instrument targeted at a handful of designated firms would be a better tool for strategic autonomy than genuinely horizontal instruments.

The Task Force considered it essential to keep the legal question, on which the non-discriminatory character of the DMA is reasonably clear, distinct from (i) the political-

economy question, on which the concentration of designated firms in one jurisdiction gives the discriminatory-effect argument real traction, and from (ii) the strategic question of whether the DMA should be pressed into service as an instrument of sovereignty at all. Managing these perceptions – through transparent enforcement, even-handed treatment of any EU firms that cross the thresholds, and clear evidence of benefit to European consumers and businesses – is itself part of making the regime durable in a hostile geopolitical climate.

4.5. UNINTENDED EFFECTS: PROPORTIONALITY, PRIVACY, SMES, AND THE INNOVATION TRADE-OFF

A distinctive contribution of the stakeholder roundtable was a detailed account, from the regulated firms and their business users alike, of the DMA's unintended or contested effects, which the Task Force considered important to record even where members did not endorse every claim.

Gatekeeper representatives argued that the DMA lacks an explicit proportionality test and adequate safeguards for intellectual property, security, and privacy. They cited interoperability requirements said to force the sharing of sensitive data, such as decrypted notifications or connection histories, in ways they regarded as less privacy-preserving than alternatives they had proposed. An industry economist made the more general point that openness and security involve a genuine trade-off that the DMA does not squarely acknowledge (Hacker et al., 2023). A retailer subject to the regime argued that designating a single large player in a market where much larger national and offline competitors are not designated distorts competition rather than correcting it. This participant added that the DMA has not delivered the single-market harmonisation it promised where national gatekeeper-style regimes, notably in Germany, apply overlapping but different rules to the same conduct (Koenig, 2025).

Representatives of smaller firms welcomed the DMA's ambition but reported that many SMEs are unaware of their rights. They contended that self-preferencing persists in practice through the control of ranking even where explicit self-preferencing is prohibited, and that dependence on gatekeeper-run logistics and services leaves them exposed to unilateral changes in terms. Several argued that the Platform-to-Business Regulation, which provides baseline protections in dealings with non-gatekeeper platforms, should be retained rather than repealed in the name of simplification.

A concrete illustration of the difficulty of judging outcomes came from the self-preferencing case concerning search: restricting a gatekeeper from surfacing its own mapping and similar services was reported to have reduced traffic to some small tourism and retail businesses. For some queries, merely shifting traffic to other large

intermediaries that are themselves gatekeepers, raises the question of whether contestability had genuinely increased.

The Task Force drew no single conclusion from these accounts, but took from them a clear message: the DMA's effects are heterogeneous and sometimes in tension with its own goals. A serious evaluation must be equipped to detect not only intended benefits, but also unintended consequences.

4.6. INTERACTIONS WITH COMPETITION LAW, OTHER INSTRUMENTS, AND GENERATIVE AI

The DMA does not operate in isolation, and the Task Force returned repeatedly to its interaction with the rest of the digital and competition *acquis*.

The DMA is intended to complement rather than displace Articles 101 and 102 TFEU and the national competition regimes, but the boundary is not always crisp (Cr mer et al., 2023; McIntyre, 2023). The parallel German regime illustrates the risk of divergent obligations for the same conduct (Koenig, 2025).

The interface with data protection law is particularly noteworthy. A representative of the European Data Protection Supervisor explained that, although data protection authorities have no role in DMA enforcement, the DMA is expressly without prejudice to the GDPR, and that joint guidelines on the DMA-GDPR interplay had been consulted. The participant pointed out that the Commission has a treaty-based duty to consult data protection authorities where its investigations touch GDPR-relevant matters, an overlap that is expected to grow (Hacker et al., 2023; Elizalde, 2025).

The same participant described the DMA's high-level group as a useful but necessarily general coordination forum, explicitly barred from advising on enforcement. The speaker proposed both a broader regulatory forum spanning digital-services, cybersecurity, and other authorities, and a legal basis for sharing information across authorities during investigations, subject to safeguards for defendants. Several participants agreed that effective coordination on specific cases, rather than high-level generality, is not possible under the current framework.

Practical questions of proportionality and treatment also surfaced, from the treatment of tying, bundling, and super-apps (Jafarguliyev, 2025; Vezzoso, 2024) to the observation that newer regimes in Japan, the UK, and elsewhere have incorporated stronger proportionality tests and procedural safeguards, which some participants urged the EU to study.

Looking forward, the rapid integration of generative AI into core platform services raises questions the drafters did not squarely confront:

- whether AI assistants, and the bundling of AI capabilities into designated services, will become vectors of entrenchment or of contestability;
- whether the current list of core platform services captures them; and
- how interoperability or data-access remedies could even be verified for services that are deeply personalised to a single customer's data (Yasar et al., 2024).

Business users pressed the related point that DMA assessment is conducted against a static snapshot of the market while services continue to innovate, so the framework must accommodate ongoing change rather than freeze a moment in time.

4.7. INSTITUTIONAL ARCHITECTURE: TOWARDS A EUROPEAN SYSTEM OF DIGITAL REGULATORS?

Finally, the discussions raised a structural question that connects the DMA to the wider governance of the digital rulebook and to Section 8 on the better regulation process. A prominent argument advanced to the Task Force was that the current arrangement, in which the Commission acts simultaneously as geopolitical executive and as digital regulator, sits uneasily with the independence normally valued in economic regulators. It was correct, in this view, to vest initial enforcement in the Commission to avoid years of delay, but the time has come to consider separating the roles.

The specific proposal was a European system of digital regulators, modelled on the European System of Central Banks and on financial supervision, pairing a strong, independent European agency with national regulators that retain field-level expertise. Interlocutors noted the obstacle that each recent digital law has its own distinct coordination mechanism, and that the DMA high-level group, while a useful network of networks, is widely regarded as pitched too high to be effective. A natural first step, several suggested, would be to extend that group's mandate beyond the DMA to the wider digital rulebook.

This institutional question recurs in the discussion of the DSA's fragmented enforcement, and the Task Force considered that the case for a more coherent architecture for European enforcement, whatever its eventual form, is one of the more important cross-cutting lessons of the first years of the DMA and DSA alike (Bruegel, 2025).

4.8. DATA ACCESS AND THE ROLE OF VETTED RESEARCHERS

Directly connected to the difficulty of measuring effectiveness, the Task Force noted that rigorous independent evaluation of the DMA will require access to data that today sit almost entirely with the gatekeepers. Yet, the DMA, unlike the DSA, contains no structured mechanism for independent-researcher access. Participants involved in the evaluation identified this absence as a concrete obstacle to a credible assessment, since compliance report data are of inconsistent quality and application programming interface (API) access varies.

The DSA has created a mechanism under which vetted researchers may access platform data to study systemic risks, and there could be scope for an analogous, carefully bounded route under the DMA to support independent assessment of contestability and fairness (Hornkohl, 2024; Hacker et al., 2023; Etteldorf, 2022). Any such mechanism would need robust safeguards for commercially sensitive information and personal data, and would have to avoid disproportionate new burdens. Still, the underlying principle, that those charged with evaluating the regime should not depend solely on the regulated firms for the evidence on which that evaluation rests, is sound, and it aligns the DMA with the more transparent evidentiary model already emerging under the DSA.

Recommendation 3. The Commission should examine whether a bounded data-access mechanism for vetted researchers, modelled on Article 40 of the Digital Services Act, could support independent evaluation of the effects of the Digital Markets Act on contestability and fairness – subject to strict safeguards for confidentiality and data protection, and to a proportionate assessment of the burden imposed.

5. FUNDAMENTAL FREEDOMS: THE DIGITAL SERVICES ACT

Key findings

The DSA has put in place an ambitious, layered supervisory architecture combining direct Commission oversight of the largest platforms with national Digital Services Coordinators, but in its first years enforcement has been fragmented and incomplete. Several Member States were late to designate or fully empower their coordinators, and some have been referred to the Court of Justice.

Effective enforcement is an essential component of regulatory credibility and compliance; however, fines are a poor measure of the DSA's success. Meaningful evaluation requires indicators of compliance quality, transparency, and content-moderation outcomes. The instruments to measure these robustly are still immature.

Recognised international assurance standards such as the IAASB's ISAE 3000 (Revised) can be employed for the independent audits required of very large online platforms, and are already used in practice. But there is not yet a dedicated, DSA-specific audit standard or commonly accepted audit methodology. This may limit comparability across engagements as well as the evidentiary value of audit outcomes, and likely increases compliance costs.

The heaviest DSA burdens fall on the large firms that are very large online platforms (VLOPs) and search engines (VLOSEs); nonetheless, the compliance burdens of the remaining obligations may represent a significant cost for SMEs inasmuch as they have to fund them out of a smaller revenue stream.

Overlaps with the GDPR, consumer law, and other instruments create uncertainty about competence and about whether data protection authorities are equipped to supervise content moderation at scale.

The Article 40 mechanism for vetted-researcher access to platform data is a genuine advance and the model to which the DMA discussion looked, but its value will depend on whether the vetting and access procedures prove workable in practice.

The Digital Services Act (Regulation (EU) 2022/2065) establishes horizontal rules for intermediary services, layering obligations according to the type and size of the service. The most demanding requirements (systemic-risk assessment and mitigation, independent audit, transparency reporting, recommender-system transparency, and data access) are reserved for VLOPs and VLOSEs (European Commission, 2026e; Moravcová, 2023). Its supervisory design is deliberately layered: the Commission enforces the

additional obligations on the very largest players directly, while national Digital Services Coordinators (DSCs) supervise the remainder and anchor the system within each Member State (Yurukova, 2025; Mattioli, 2025).

The DSA thus pursues a difficult balance: protecting fundamental freedoms (above all, freedom of expression and information) against the systemic risks posed by the largest platforms, while avoiding the imposition of disproportionate burdens on smaller actors and preserving the single market. The first years of operation have demonstrated both the promise of this architecture and the practical difficulty of making it function coherently across 27 Member States.

5.1. ENFORCEMENT FRAGMENTATION AND THE DIGITAL SERVICES COORDINATORS

The DSA deliberately leaves Member States considerable freedom in how they organise their competent authorities. While this respects national institutional traditions, it creates a standing risk of fragmentation and places a heavy premium on the duty of sincere cooperation between national authorities and the Commission (European Law Blog, 2023; Mattioli, 2025).

The most immediate concern is that there is no enforcement body in place and no trusted flaggers designated in some Member States. This reflects a real and documented implementation gap. A number of Member States were slow to designate or fully empower their DSCs, and the Commission has referred several of them to the Court of Justice for failing to do so (European Commission, 2026c).

The first annual reports of the DSCs, analysed shortly after publication, revealed uneven capacity across Member States. A marked concentration of cross-border complaints was apparent in the small number of jurisdictions where the largest platforms are established, along with the slow activation of trusted flaggers and bodies for out-of-court dispute settlement (The Platform Law Blog, 2025; Yurukova, 2025). Independent surveys of the enforcement landscape have described a system at a crossroads, with fragmentation, uneven resourcing, and political resistance all in evidence (Centre for Future Generations, 2026).

Understaffing compounds these problems directly: a coordinator that lacks the personnel and technical expertise to scrutinise platform behaviour cannot supervise effectively, however well drafted its mandate.

This diagnosis has prompted proposals for a more centralised solution, up to and including a dedicated EU digital enforcement authority modelled on bodies such as the European Securities and Markets Authority (Bruegel, 2025). The Task Force considered such an agency well worth serious study, and it connects directly to the discussion, in Section 8

on the better regulation process, of a possible single market agency drawing on seconded national expertise. At the same time, Task Force participants were realistic about the institutional and political obstacles to creating one.

Recommendation 4. The Commission and Member States should give priority to closing the implementation gap for the Digital Services Act, ensuring that every Digital Services Coordinator is designated, sufficiently resourced, and fully empowered. It should formally evaluate whether a more centralised enforcement body, drawing on seconded national expertise, would raise the effectiveness and consistency of enforcement. There is a need not only for better and faster implementation, but also for improved coordination across enforcement levels.

5.2. MEASURING WHAT MATTERS: TRANSPARENCY AND CONTENT-MODERATION OUTCOMES

A central point of agreement was that, while effective enforcement is an essential component of regulatory credibility and compliance, fines are not the right metric for measuring the DSA's success. The regulation's purpose is to reduce systemic risks and to improve the quality, consistency, and accountability of content moderation and platform governance, not to generate penalties. An enforcement record measured principally in fines could even indicate failure, in the sense that harm had already materialised, rather than success (Monti, 2024; Eder, 2024). Yet the indicators that would permit a better assessment – the accuracy and consistency of moderation decisions, the meaningfulness and comparability of transparency reporting, the effectiveness of notice-and-action and internal complaint-handling, and the responsiveness of out-of-court redress – are still being developed and standardised (Leerssen, 2023; Wei et al., 2024; Ortolani, 2023).

Work on operationalising the very notion of moderation accuracy shows how much conceptual and methodological groundwork remains before such outcomes can be measured reliably (Wei et al., 2024). Transparency rights, including the obligation to give reasons for moderation decisions and the resulting statements-of-reasons database, offer a foundation. But early empirical comparison of the DSA transparency reporting by platforms with independently observed behaviour has found notable inconsistencies, underlining the need for standardised and verifiable metrics rather than self-declared figures (Sekwenz et al., 2026; Leerssen, 2023).

Broader analyses of content governance at scale, and of the systemic-risk framework that is the DSA's most novel instrument, reinforce the point that the regulation's success or failure will be intelligible only through carefully designed outcome indicators (Bagonza, 2026; Eder, 2024). The transparency database and the work of the European Centre for

Algorithmic Transparency provide institutional starting points, but the Commission should invest in agreed, comparable outcome indicators for content moderation and systemic-risk mitigation, and treat their development as a core supervisory task rather than a by-product.

Recommendation 5. The Commission, working with the Digital Services Coordinators and the European Centre for Algorithmic Transparency, should develop and publish a common set of verifiable outcome indicators for content moderation and systemic-risk mitigation, so that compliance can be judged on comparable evidence rather than on the platforms' self-declared figures or on the level of fines imposed.

5.3. AUDIT STANDARDS AND RESEARCHER DATA ACCESS

Two structural gaps deserve particular attention because they concern the machinery through which the DSA is supposed to generate reliable evidence.

First, the DSA requires very large platforms to undergo independent annual audits of their compliance. Recognised international assurance standards such as the IAASB's ISAE 3000 (Revised) can be employed and are already used in practice; however, there is not yet a dedicated DSA-specific audit standard or commonly accepted audit methodology. This may limit comparability across engagements as well as the evidentiary value of audit outcomes, and likely increases compliance costs (Freshfields, 2026).

Second, the mechanism for vetted-researcher access to platform data under Article 40, given operational form by the associated delegated regulation, is a genuine advance, and, notably, the very model to which the Task Force's DMA discussion looked for inspiration (Keller, 2025; European Commission, 2025a; Hogan Lovells, 2025). A substantial body of scholarship has examined both its promise, as a remedy for the information asymmetry that has long hampered platform research and systemic-risk supervision, and its practical limitations, including the complexity of the vetting procedure and the scope for platforms to resist or delay (Liesenfeld, 2024; Goanta et al., 2025; Greser, 2024).

Early accounts of the mechanism in operation, including its use in election-related research, describe both real progress and considerable friction (Ohme & Seiling, 2026; Darius et al., 2026). The value of Article 40 will ultimately depend on whether the vetting and access procedures prove workable for bona fide researchers without creating disproportionate risks to security or personal data.

Recommendation 6. The Commission should support the development of additional guidance, criteria, and best practices for the independent audits required under the Digital Services Act, building on existing assurance frameworks such as ISAE 3000 (Revised), with the aim of promoting greater consistency, comparability, and evidentiary value across audit engagements. The Commission should actively monitor the operation of the Article 40 data-access mechanism, standing ready to streamline the vetting and access procedures if they prove unworkable in practice for bona fide researchers.

5.4. COMPLIANCE COSTS, SMES, OVERLAPS, AND DEFINITIONAL SPILLOVER

The Task Force also noted the distributional dimension of the DSA. Although the heaviest obligations are reserved for the largest and most impactful platforms (VLOPs and VLOSEs), the compliance burden of the horizontal rules falls proportionally harder on smaller providers, for whom the fixed costs of legal interpretation, tooling, and reporting loom larger. SME concerns are not always sufficiently reflected in implementation (Moravcová, 2023; Smith, 2025).

A recurring theme, developed further in Section 8 on the better regulation process, is that overlaps with other instruments generate uncertainty and cost. The DSA intersects with the GDPR, with EU consumer law, and with the DMA, and the resulting overlap of applicable rules and competent authorities can leave firms unsure which regime governs a given situation and which authority will enforce it (Elizalde, 2025; German Marshall Fund of the United States, 2025).

A specific concern raised in Task Force discussions is whether data protection authorities, whose expertise lies in the GDPR, are equipped to supervise content moderation at scale. Another is whether concepts developed for the DSA and DMA are being borrowed and misapplied in adjacent contexts. Both point to the need for careful coordination among authorities and for discipline in the use of defined terms across the *acquis* (Elizalde, 2025).

As with the DMA, the DSA is not discriminatory in design in the sense that its provisions do not literally discriminate. Yet its concentration of direct enforcement on a small number of large, mostly non-EU platforms invites the same discriminatory-effect critique, and the same need to manage that perception through transparent, evidence-based enforcement (German Marshall Fund of the United States, 2025).

6. THE ARTIFICIAL INTELLIGENCE ACT

Key findings

The AI Act's risk-based architecture commands broad support in principle, but its operation depends on harmonised standards, guidance and codes of practice that are not yet fully in place, leaving providers uncertain how, in concrete terms, to comply.

As with other EU laws, there is scope to simplify the AI Act, and portions of the Digital Omnibus already seek to begin the job; however, it will nonetheless be important to continue to safeguard the AI Act's objectives relating to fundamental rights, safety, and trust. The Task Force saw the central challenge not as a binary choice between deregulation and stricter rules, but as the provision of practical, example-based guidance that confers legal certainty without becoming over-prescriptive.

Legislators frequently lack the operational, technical expertise that resides mainly within industry, and the better regulation process does not yet reliably capture it. Several participants argued for broader input, including from the social sciences and humanities.

The General-Purpose AI Code of Practice and the AI Office are important steps, but the AI governance system remains incomplete, and a third instrument originally intended to address AI liability is absent.

The 2025–26 simplification effort, through the Digital Omnibus and the subsequent agreement to streamline the Act, postpones certain obligations and lightens others, but leaves the core requirements substantively unchanged. Changes to substance should be grounded in evidence and, where material, in proper impact assessment.

The Artificial Intelligence Act (Regulation (EU) 2024/1689) is the most ambitious attempt yet to regulate AI horizontally. It classifies systems by the level of risk they present, prohibiting a small set of practices outright, imposing detailed obligations on systems designated as high-risk, adding lighter transparency duties for certain other systems, and establishing a dedicated regime for general-purpose AI (GPAI) models (European Commission, 2026a; Gstrein et al., 2024; Revolidis, 2025).

Because the Act was the principal focus of the Task Force's fourth meeting, and because its implementation has progressed rapidly since then, this section draws directly on that discussion, and on the contributions of individual participants, as well as on the wider literature. The overarching mood of the discussion was not hostility to the Act's objectives but concern about implementability, expertise, and coherence, and a shared sense that

the difficult work lies less in the statute than in the guidance, standards, and institutions that must give it practical effect.

6.1. THE RISK-BASED APPROACH AND ITS CRITICS

The risk-based approach is widely accepted, and much of the scholarly debate concerns not whether to use it but how to implement it well (Elbers, 2024; Justo-Hanani, 2025). Two lines of criticism recur. The first questions whether a framework rooted in product-safety logic and self-assessment can adequately protect fundamental rights, and whether the fixed, category-based list of high-risk uses can keep pace with a technology that is evolving faster than the classification (Kusche, 2024; Popović & Vujičić, 2026; Nannini, 2025). A second line argues that the Act is, in important respects, underspecified for generative and general-purpose systems, whose broad and unpredictable range of downstream uses does not map neatly onto the original risk tiers (Revolidis, 2025). They were added to the AI Act at the last minute, with complex rules on allocation of responsibility in the value chain.

Proposals to move from a categorical to a more contextual understanding of high-risk classification, and comparative work drawing on other jurisdictions' emerging approaches, indicate that the design of the risk tiers will remain contested well into the implementation phase (Nannini, 2025; Bang, 2026; Kim & Ko, 2026). The Task Force's own discussion, however, was less preoccupied with the architecture of the tiers than with the lived experience of trying to comply with them, and it is to that experience that the most distinctive contributions of the fourth meeting were directed.

6.2. SIMPLIFICATION, GUIDANCE, AND THE SECTORAL DIMENSION

A central intervention came from a guest speaker who cautioned against equating simplification with the mere removal of normative obligations. In her account, framing the Digital Omnibus principally as a reduction in obligations misdiagnoses the problem: what companies and public bodies most lack is specific guidance on how to apply the obligations that already exist. Some measures presented as simplification could in practice make compliance more, rather than less, complicated. She proposed two complementary remedies. The first was to codify and consolidate AI-related norms across the digital *acquis*, so that the applicable rules are easier to locate and reconcile. The second was a systematic revision of the sector-specific EU legislation that intersects with the AI Act, so as to concretise how the Act's requirements apply in particular contexts, rather than adding yet more articles to the Act itself.

She illustrated the point from the health sector, observing that the AI Act's research-and-development exemption does not extend to real-world testing, which makes it very difficult for hospitals and clinical settings to meet robustness and accuracy requirements.

She noted, by way of contrast, that instruments such as the Cyber Resilience Act supply the concrete technical standards that the AI Act leaves unspecified. This concern, that the Act's high-level requirements need to be operationalised through sectoral standards and interdisciplinary implementation, is strongly echoed in the literature on medical and other high-risk applications (Montag & Finck, 2024; Zhong, 2024; Värri, 2025; Aboy et al., 2024).

6.3. GUIDANCE WITHOUT PRESCRIPTION, AND THE EXPERTISE GAP

A theme that united several interventions was the search for a workable middle ground between rigid, exhaustive rules and open-ended flexibility.

One participant argued that the AI Office's guidance on prohibited practices, which relied on illustrative examples rather than attempting to specify every case, was a good model. It offered legal certainty without being over-prescriptive, which is especially valuable in a fast-moving field where expertise is scarce and where overly narrow rules risk being overtaken by events.

The same participant also drew attention to a structural tension in the whole enterprise. Much of the operational, practical expertise needed to regulate AI well resides within private companies, which cannot themselves make law without raising obvious concerns about democratic legitimacy. The implication is that the better regulation process, through consultation and evidence-gathering, must do a far better job of extracting the right expertise from among a very large number of stakeholders.

Another participant made a complementary point, arguing that the complexity of the issues, including culturally freighted questions about the representation of the human body in art, literature, and film, calls for the involvement of experts from the social sciences and humanities, not only technologists and lawyers. The chair gave a clear illustration of the same expertise gap: non-expert legislators risk producing very detailed rules on matters they do not fully understand, such as the debate over 'nudification' tools. A participant further warned that a regulatory posture dominated by prohibitions risks discouraging innovation and deterring international partners, some of whom, he reported, prefer to avoid EU-style regulation altogether so as not to slow their own pace. He also questioned whether the EU's enforcement capacity matched its regulatory ambition, given that governmental and business attention is increasingly focused on competitiveness and on strategies such as Apply AI.

The chair framed the underlying dilemma as one of timing: regulate too late and harmful patterns become entrenched, regulate too early and one risks betting on the wrong horse and inhibiting innovation – a judgement that is inherently case-specific. These concerns about expertise, interdisciplinarity, and the practical difficulty of implementation are

widely shared in the scholarly literature (Montag & Finck, 2024; Zhong, 2024; Drage et al., 2025; Fernández-Llorca et al., 2024).

6.4. GOVERNANCE, STANDARDS, AND THE GENERAL-PURPOSE AI CODE OF PRACTICE

On governance, the Task Force welcomed the establishment of the AI Office and the associated scientific panel and advisory bodies, while stressing that their effectiveness will depend on sufficient resources and expertise and on the timely delivery of harmonised standards by the European standardisation organisations (Novelli et al., 2024; Parisini & Dervishaj, 2025). The dependence on harmonised standards is more than a technicality: until those standards exist, providers of high-risk systems face genuine uncertainty about what compliance concretely requires. The standardisation process has itself been identified as a bottleneck and a locus of implementation risk (Kilian et al., 2025; Värri, 2025).

The General-Purpose AI Code of Practice, published in 2025 with chapters on transparency, copyright, and safety and security, was seen as a pragmatic bridge for the period before harmonised standards are available, offering GPAI providers a voluntary route by which to demonstrate compliance with their obligations (European Commission, 2025b; Jones Day, 2025; Farrell & Emborg, 2025). The Code, and the GPAI regime more broadly, have attracted close analysis, including of the treatment of systemic-risk models, of copyright, and of the interaction with open-source models. The debate over how prescriptive the Code should be mirrors the broader tension between guidance and prescription identified above (Revolidis, 2025; Kontosis & Davalas, 2026; Ramos & Pianese, 2026).

Regulatory sandboxes, intended to give innovators, and especially SMEs, a supervised space in which to develop and test AI systems, were noted as a potentially important tool whose value will depend heavily on how well they are designed and governed in practice (Ahern, 2025; Novelli et al., 2026; Genicot, 2026).

6.5. AI AND LIABILITY

A distinct concern, raised by CEPS, was that the AI governance system arguably remains incomplete. The original design envisaged three interlocking instruments: the AI Act itself, a revised Product Liability Directive, and a dedicated AI Liability Directive allocating responsibility for harm caused by AI systems. With the withdrawal of the proposed AI Liability Directive, only two of the three are in place, potentially leaving a gap in the civil-liability framework that the third instrument was meant to fill.

The Task Force heard that work is under way to develop a comprehensive proposal to plug this gap, drawing on international scholarship, industry, and civil society, with a view to ensuring that the overall system of AI governance functions coherently rather than partially. Resolving the allocation of liability matters not only for the protection of those harmed but also for legal certainty for developers and deployers, and it bears directly on the coherence of the framework as a whole.

Support for an AI liability pillar is by no means universal. A number of prominent industry associations have jointly argued that an AI Liability Directive would be needlessly burdensome (Industry Associations, 2025).

6.6. SIMPLIFICATION IN PRACTICE: THE DIGITAL OMNIBUS AND THE STREAMLINING OF THE ACT

The Act is already being amended in the name of simplification. The Digital Omnibus on AI was proposed in late 2025 as a response to the competitiveness agenda set out in the Draghi report and the subsequent agreement between the Council and Parliament in 2026 to streamline the Act. It postpones certain high-risk obligations, lightens some requirements, centralises elements of implementation in the AI Office, and introduces measures such as an EU-level sandbox (European Commission, 2026b; Council of the European Union, 2026; Tech Policy Press, 2026a; Morrison & Foerster, 2025).

The prevailing assessment is that these changes adjust timing and administration while leaving the Act's core requirements substantively intact (Tech Policy Press, 2026a; Gartner, 2025). Commentators have nonetheless cautioned against conflating two distinct things: legitimate implementation support, such as filling gaps in standards, designating competent authorities, and clarifying obligations, on the one hand, and substantive regulatory relief presented under the banner of simplification, on the other (AI Act Blog, 2026; Dignum et al., 2026). This distinction matters a great deal, and it connects to the Task Force's wider concern, developed in Section 8 on the better regulation process, about omnibus proposals being advanced without impact assessment.

Task Force participants seemed to feel, consistent with their views on simplification as noted elsewhere in this report, that lightening the genuine administrative burden is welcome and overdue, but that changes to the substance of the Act, as opposed to its timing or its paperwork, should be grounded in evidence. Where significant, they should be supported by a proper impact assessment, rather than adopted under a general and largely unexamined banner of urgency.

Recommendation 7. The Commission should give priority to completing the AI Act's overall implementing architecture, the harmonised standards and practical, example-based guidance that give providers legal certainty. There may well be a need to also clarify AI liability.

Recommendation 8. Amendments pursued under the simplification agenda should distinguish clearly between administrative streamlining and substantive change. Any substantive change should be supported by evidence and, where material, by an impact assessment, rather than justified by an unexamined appeal to urgency.

7. PRIVACY, CYBERSECURITY, AND DATA SHARING

Key findings

The GDPR is rightly called Europe's regulatory gold standard. Gold is precious, but it is also heavy.

Arguably, the GDPR pays too little attention to the EU legislative principle of *proportionality*, or to the *balancing of privacy interests with other interests*. There is a single recital, but no operative text to implement it.

The GDPR's *one-stop shop* (where enforcement mainly falls to the Member State in which a firm has its EU headquarters) is problematic in that (i) it saddles two of the smallest Member States with most of the large-scale actions challenging enforcement, and (ii) the responsible Member State may be subject to a conflict of interest.

The Commission submitted a Digital Omnibus ostensibly in an effort to simplify the GDPR. It seeks to simplify cookie rules – a long overdue reform. The Digital Omnibus also seeks to refine standards for pseudonymisation and to redefine what constitutes personal data, which is a contentious change. The more fundamental problems in the GDPR, such as insufficient attention to proportionality, a flawed one-stop-shop approach, and too much complexity overall, remain to be tackled in future legislation.

Still, like all omnibus proposals, the Digital Omnibus was put forward without an impact assessment. The European Parliament has decided to conduct its own impact assessment, which is now ongoing.

Multiple EU laws govern data transfer and portability, including the GDPR, the Data Act, and DMA. These provisions do not appear to be fully mutually consistent.

The Network Information and Security Directive (NIS 2), Cyber Resilience Act, Digital Operational Resilience Act (DORA), and the forthcoming Digital Networks Act collectively represent the most ambitious attempt yet to build a coherent European cybersecurity architecture that reduces systemic vulnerabilities, strengthens resilience, and enhances technological sovereignty.

But the current governance model remains fragmented, duplicative, and operationally burdensome, particularly for entities subject to multiple sectoral regimes. This stems from the accumulated complexity of overlapping obligations, inconsistent definitions, and divergent enforcement practices. Overlaps are everywhere, but are especially

prominent between horizontal cybersecurity legislation and sector-specific frameworks, for instance in health, finance, and digital infrastructure.

The Digital Omnibus seeks to consolidate incident-reporting obligations across multiple EU laws – a worthy goal. It may not go far enough in standardising definitions, reporting time frames, or incident-severity definitions. Whether this is politically feasible remains to be seen.

Aligning EU cybersecurity and privacy laws is challenging because the laws embody divergent regulatory philosophies. NIS 2 is fundamentally risk based, focusing on operational resilience and incident response. The CRA is safety based, oriented towards product conformity and lifecycle security. The GDPR's breach-notification rules are grounded in fundamental rights protection. The European Health Data Space introduces sector-specific data governance obligations. Harmonising these regimes is inherently difficult because they pursue different objectives and apply different conceptual frameworks.

7.1. PRIVACY: THE GENERAL DATA PROTECTION REGULATION AND DIGITAL OMNIBUS

The GDPR¹ is often referred to as Europe's regulatory gold standard, and there is much to be said for this. An integrated standard for all 27 Member States is greatly preferable to (for instance) privacy regulation in the US, which is fragmented both state by state and sector by sector, with many sectors not at all covered by law at the US federal level.

In acknowledging the GDPR as the EU's regulatory gold standard, we must not forget that while gold is precious, it is also heavy. Large numbers of stakeholders view the GDPR as needlessly burdensome. Many Europeans are suffering from 'consent fatigue', and most are sick and tired of cookie banners.

In addition to these consumer-visible problems, there are further challenges. GDPR legislation pays to little attention to the EU legislative principle of *proportionality*. Recital 4 GDPR states clearly: 'The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.' This, however, is the only reference to proportionality in the GDPR, and there is no operative text

¹ Data held by the EU or its agencies is excluded from the scope of the GDPR. It is covered instead by a separate regulation, the *EUDPR*. The EUDPR is similar in structure and content to the GDPR. In the interest of simplicity, we do not separately address the EUDPR; the issues raised are generally a subset of those relevant to the GDPR.

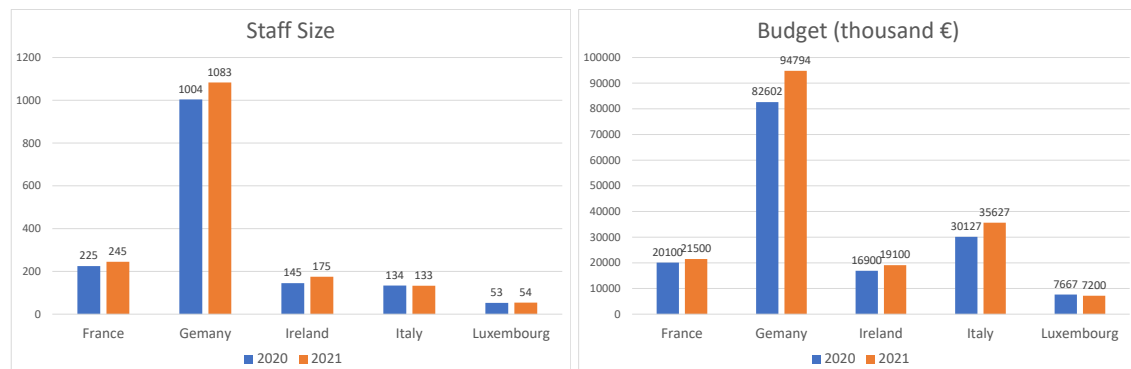
whatsoever to operationalise the principle, nor enumeration of the other fundamental rights that should be considered, or the function that the protection of personal data plays in society. As a result, court decisions and those by the European Data Protection Board (EDPB) arguably pay far too little attention to anything other than the protection of personal data.

This problem is exacerbated by the fact that there is no explicit provision for appealing EDPB decisions. EDPB decisions are extremely difficult to appeal because they are not addressed to individuals or companies, and only the Member State data protection authorities formally involved in the dispute can challenge them. This creates a structural accountability gap: once the EDPB adopts a binding decision, proportionality concerns raised by affected parties have almost no procedural route to judicial review.

A second serious problem in the GDPR is its *one-stop shop*. The *data protection authority* in the Member State where a firm has its EU headquarters is responsible for all enforcement actions against the firm (with minor exceptions due to a case brought by Belgium). Consider that of the five big tech ‘GAFAM’ firms, four have their EU headquarters in Ireland and a fifth in Luxembourg. These five firms provide a substantial fraction of all of the digital services offered worldwide. The one-stop shop implies that most of the hard cases must be handled by two of the smallest Member States – a clearly inappropriate use of resources.

Calculations by the EDPB in 2021 (European Data Protection Board, 2021) seem to suggest that while Ireland and Luxembourg have allocated significant resources in terms of staff size and budget (see Figure 2), the resources assigned are nonetheless probably not commensurate with the job that these two Member States have to do. Ireland and Luxembourg have devoted progressively greater resources since 2021, but it is likely that their combined staff and budget are still only about an eighth of total EU staffing. In other words, the staff and budgetary resources they have deployed are still far from being commensurate with the burden of responsibility for the bulk of the GDPR’s one-stop-shop supervision of big tech firms (mainly Meta, Google, Apple, Amazon, TikTok, and Microsoft) in the EU27.

Figure 2. GDPR enforcement staff size and budget, selected Member States (2020–21)



Source: EDPB (2021) and author's calculations.

One must also wonder whether these Member States, which worked hard to obtain those corporate headquarters, will be highly motivated to act expeditiously against the firms.

The Commission recently submitted a Digital Omnibus proposal (2025/0360(COD)), ostensibly as a means of simplifying the GDPR and several other EU laws.

The main simplifying measure is an attempt to consolidate the cookie rules (currently spread across the ePrivacy Directive and GDPR) so that they are together in the GDPR, and to begin to create standards so that the user is only forced to respond once every several months. These revisions seem to be promising, and offer a genuine prospect of simplification; however, the measure leaves the cookie rules in place under Article 5(3) of the ePrivacy Directive insofar as they relate to non-personal data. A single cookie may relate to both personal and non-personal data. There is a strong argument to be made that the consolidation of cookie rules into the GDPR should have been comprehensive, rather than leaving a split regime to persist.

At the same time, a number of industry associations have expressed concerns that the Digital Omnibus as ultimately enacted may not achieve enough simplification – it might be watered down too much along the way (Industry Associations, 2026).

The other major change to the GDPR through the Digital Omnibus consists of refinements to the definitions of anonymisation, pseudonymisation, and personal data overall. These may be useful, particularly for laws such as the **European Health Data Space**, where the use of anonymised or pseudonymised '*secondary data*' for research and public health purposes might have been at risk of judicial challenges. All the same, these are changes with far-reaching consequences. Changes this broad would normally be appropriate after detailed analysis by the Commission, which was not done. We discuss these points in greater detail in Section 7.2.

The Digital Omnibus, like all of omnibus regulatory proposals, was submitted without an *impact assessment*. The Commission has sought to justify this omission (i) due to urgency, (ii) because the changes in the omnibus proposals are purely technical, and (iii) because the omnibus proposals do not constitute standalone legislation – they are only amendments to existing laws.

The European Ombudsperson did not see things that way. The Ombudsperson found that the Commission's claim of urgency was not appropriately justified, and also directed the Commission to establish a procedure as to which steps could be omitted in cases where urgency is truly justified. In a case involving Omnibus I (for the Corporate Sustainability Reporting Directive, Corporate Sustainability Due Diligence Directive, and Taxonomy) and two other laws, the Ombudsperson issued a finding of *maladministration* on the part of the Commission (Marcus, 2026). As regards Omnibus I, the findings are fully in line with Marcus & Thomadakis (2025).

The European Parliament has concluded that the change in the definition of personal data, while not necessarily wrong, was too complex in its implications to wave through without an impact assessment. Hence, Parliament will conduct its own impact assessment of the Digital Omnibus.

Meanwhile, the more fundamental problems in the GDPR – insufficient attention to proportionality, a flawed one-stop-shop approach, and too much complexity overall – remain to be tackled in future legislation.

Taking these various concerns all together, these issues reveal a deeper governance and accountability deficit in the GDPR's institutional architecture. Although the regulation is rightly celebrated as Europe's regulatory gold standard, it lacks the operational mechanisms needed to balance the fundamental right to data protection against other Charter rights, leaving proportionality – explicitly required by the Charter of Fundamental Rights in Article 52(1) – to be reconstructed ad hoc by courts and supervisory authorities. This gap is compounded by the absence of a meaningful appeal route for binding decisions of the EDPB, which are addressed solely to national data protection authorities and therefore largely insulated from direct judicial review by affected parties.

As discussed above, the one-stop-shop system concentrates the most complex and resource-intensive enforcement responsibilities in Ireland and Luxembourg, whose combined staffing and budgets remain only a small fraction of the total resources of the EU data protection authority, despite supervising the bulk of major cross-border cases involving Meta, Google, Apple, Amazon, TikTok, and Microsoft.

These structural imbalances – limited proportionality guidance, constrained accountability, and uneven enforcement capacity – interact in ways that systematically

weaken the GDPR's ability to deliver consistent, timely, and proportionate outcomes across the EU.

7.2. MEASURES TO IMPROVE THE SHARING OF DATA

Personal versus non-personal data

Most data-sharing arrangements in the EU have their primary focus on *non-personal data*. This is particularly true of the Data Governance Act, the Free flow of non-personal data Regulation ((EU) 2018/1807), the Open Data Directive ((EU) 2019/1024), and other current laws. This is perhaps appropriate – addressing personal data matters would entail complex issues of GDPR and EUDPR compliance.

Some laws deal with both personal and non-personal data. The EHDS, for instance, deals with not only secondary use (where anonymised or pseudonymised data are made available for use by researchers and public health authorities), but also with primary use (where patients have a right to have their electronic health records shared with other healthcare providers if, for instance, the patient would like a second opinion or a specialist opinion). Anonymised data can be treated as being non-personal; for pseudonymised data, however, the treatment depends on how practical it is for the subject to be re-identified.

This inevitably raises questions as to whether we can properly distinguish between personal and non-personal data, and whether pseudonymisation provides a sufficient basis for treating otherwise personal data as being non-personal. Some purists would argue that it is always possible to re-identify pseudonymised data, and that consequently, pseudonymised data must invariably be treated as constituting personal data.

It must also be said that firms often have difficulty determining in practice whether their data are personal or not. There is thus a strong tendency to err on the side of caution, and to act as if all data (in emails, for example) were personal data. This presumably leads to an increased compliance burden, and with it a loss of EU productivity and competitiveness.

The Digital Omnibus proposal sought to address this very real challenge by clarifying criteria for pseudonymisation, and by redefining personal data so as to exclude pseudonymised data if the recipient lacks the means (at present) to re-identify it.

Subsequent to the last Task Force meeting, we learned that Parliament is concerned that changing the definition of personal data could potentially have large implications – it is not a simple technical change. As previously noted, the Commission did not provide an adequate analysis of the impacts – in fact, none of the Commission's omnibus proposals

was accompanied by an impact assessment. (This lack was harshly criticised in Marcus & Thomadakis (2025), and also led the European Ombudsperson to issue a finding of *maladministration* on the part of Commission (Marcus, 2026)). Parliament will consequently conduct its own *targeted, substitute impact assessment* of key GDPR aspects of the Digital Omnibus, which is an important development in the evolution of better regulation practice in the EU. It has been common for the European Parliament Research Service to conduct impact assessments, but typically these are superficial documents of six to ten pages reviewing a Commission legislative proposal for internal consistency, with no reliance on external expertise and no penetrating analysis. There have been no more than a half dozen instances where Parliament has taken responsibility to conduct a serious impact assessment, supported by external expertise – usually in politically sensitive files where the Commission failed to provide an adequate impact assessment of its own.

Issues with the Data Act

Participants raised a number of concerns as regards the Data Act. Some asked whether the Data Act imposed disproportionate costs on IoT. Relatedly, others asked whether the Data Act restrictions on the transfer of non-personal data were too burdensome.

One potentially important comment reflected an apparent conflict between the Data Act, GDPR and the DMA. A data holder might be subject to data portability obligations under the GDPR, and a gatekeeper data holder might be subject to additional data portability obligations under the DMA. If, however, the intended data recipient firm is also a gatekeeper, then the data transfer that is required under the GDPR or DMA would appear to be prohibited under Article 5(2) of the Data Act. The Digital Omnibus neglected to address this apparent conflict among the laws.

7.3. CYBERSECURITY

Cybersecurity governance challenges in the EU: fragmentation, proportionality, and the limits of coordination

Stakeholder input to the CEPS Task Force highlights a broad consensus that the EU has made significant strides in cybersecurity policy over the past five years. Instruments such as NIS 2, the CRA, DORA, and the forthcoming Digital Networks Act collectively represent the most ambitious attempt yet to build a coherent European cybersecurity architecture. Stakeholders also emphasised that the impending revision of the Cybersecurity Act will be critical. NIS2, the CRA, DORA, and Digital Networks Act establish the substantive obligations of the EU's cybersecurity framework. Revision of the Cybersecurity Act, however, offers the opportunity to operationalise these instruments by strengthening

EU-wide certification, enhancing the operational role of the EU Agency for Cybersecurity (ENISA), and limiting fragmentation across national implementation practices.

These initiatives reflect the EU's strategic ambition to reduce systemic vulnerabilities, improve resilience, and increase technological sovereignty. Even so, stakeholders emphasised that the current governance model remains fragmented, duplicative, and operationally burdensome, particularly for entities subject to multiple sectoral regimes. The challenge is not the ambition of EU cybersecurity policy, but rather the risk of unintended intersection with other EU laws, potentially leading to overlapping obligations, inconsistent definitions, and divergent enforcement practices.

Fragmentation of cybersecurity obligations across horizontal and sectoral regimes

A central theme in stakeholder discussions was the misalignment between horizontal cybersecurity legislation and sector-specific frameworks. NIS 2 establishes a broad baseline for cybersecurity risk management and incident reporting across essential and important entities. Yet, many of these same entities – particularly in health, finance, and digital infrastructure – are simultaneously regulated under sectoral regimes with their own cybersecurity and reporting requirements.

The EHDS is a clear example. Most EHDS-regulated actors are also NIS 2 entities, yet the two frameworks impose parallel obligations with different reporting thresholds, timelines, and definitions of what constitutes a 'significant' or 'material' incident. This creates a dual compliance burden: entities must interpret two sets of rules, manage two reporting channels, and reconcile two sets of expectations from supervisory authorities. The problem is not merely administrative; it affects operational response. Divergent timelines and thresholds can lead to over-reporting, under-reporting, or misaligned prioritisation during incidents. Beyond establishing a common reporting deadline for all regulations covered by the single-entry point for reporting an incident from the time at which it is confirmed, and establishing common definitions for the severity of an incident, there appears to be a need to put feedback mechanisms in place. These mechanisms should enable reporting entities to flag issues regarding the functioning, reliability, or integrity of the single-entry point.

This fragmentation is not limited to the EHDS. DORA imposes detailed ICT risk-management and incident-reporting obligations on financial entities. The CRA introduces product-security requirements and vulnerability reporting obligations for manufacturers and developers. The GDPR imposes breach-notification obligations grounded in fundamental rights protection rather than cybersecurity risk. The result is a

landscape where operators may face four or five distinct incident-reporting channels, each with its own criteria, timelines, and supervisory expectations.

Participants stressed that this fragmentation is not simply inconvenient; it is structurally inefficient. It increases compliance costs, diverts resources from actual security improvements, and does not necessarily produce better situational awareness for authorities. In some cases, it may even hinder crisis response by forcing operators to prioritise reporting over remediation.

Even though EU cybersecurity is horizontal in its applicability across sectors, a basic limitation is that these measures were typically layered on top of existing laws after the fact. In principle, a shift in policymaking culture is needed so that cybersecurity considerations are integrated from the ground up whenever new law is conceptualised. In practice, however, achieving this without further increasing fragmentation is far from straightforward. Sectoral regimes have their own regulatory philosophies, supervisory structures, and political constituencies, and integrating horizontal cybersecurity requirements into these frameworks risks either duplicating obligations or creating new inconsistencies.

The limits of proportionality and prioritisation in EU cybersecurity law

Another recurring theme was the under-specification of proportionality in the EU's cybersecurity framework. While proportionality is a constitutional requirement under the Treaties, stakeholders observed that cybersecurity legislation often lacks clear operational guidance on how proportionality should be applied in practice.

NIS 2, for example, mandates 'appropriate and proportionate' technical and organisational measures, but provides limited detail on how proportionality should be assessed across sectors, entity sizes, or risk profiles. The CRA similarly requires manufacturers to implement proportionate cybersecurity measures, yet the criteria for determining proportionality remain vague. This lack of clarity can lead to rigid or overly formalistic interpretations, particularly among supervisory authorities that may default to maximalist readings of obligations.

The problem is compounded by the divergent regulatory philosophies embedded in different instruments. NIS 2 is fundamentally risk-based, focusing on operational resilience and incident response. The CRA is safety-based, oriented towards product conformity and lifecycle security. GDPR breach-notification rules are grounded in fundamental rights protection. The EHDS introduces sector-specific obligations for data governance. Harmonising proportionality across these regimes is inherently difficult because they pursue different objectives and apply different conceptual frameworks.

Proportionality is not a request for deregulation, but for better-targeted regulation. Without clearer guidance, entities face uncertainty, authorities face inconsistent enforcement, and the overall system becomes less predictable.

Accountability gaps in EU-level coordination structures

Stakeholders also highlighted concerns about accountability and procedural fairness in emerging EU-level bodies for cybersecurity coordination. The European Cybersecurity Competence Centre, ENISA, and proposed crisis-governance mechanisms under the Digital Networks Act are expected to play increasingly influential roles in shaping cybersecurity policy, coordinating incident response and issuing guidance.

Operators noted that these bodies often wield significant influence but the procedural routes for challenging decisions or seeking review when obligations appear disproportionate or operationally infeasible are uncertain. This creates a structural accountability gap: decisions that materially affect operators may not be accompanied by accessible mechanisms for redress. Stakeholders stressed that as EU-level coordination expands, accountability mechanisms must expand with it. The forthcoming revision of the Cybersecurity Act offers a key opportunity to operationalise these coordination structures and better align their growing responsibilities with clear procedural safeguards.

Consolidated reporting: ambition vs political feasibility

One of the most concrete participant concerns was the fragmentation of incident-reporting obligations and the political feasibility of consolidating them. The Digital Omnibus package aims to streamline reporting across NIS 2, DORA, the GDPR, and CRA by taking preliminary steps to align definitions, thresholds, and timelines. Participants broadly support this ambition, viewing consolidated reporting as essential for reducing administrative burden and improving situational awareness, but note that much more work will be needed to achieve meaningful alignment.

They also expressed strong doubts about the political feasibility of meaningful consolidation. Member States view incident reporting as a core sovereign function, closely tied to national security, sectoral oversight, and crisis management. As a result, they are reluctant to harmonise thresholds or surrender sector-specific discretion – particularly in sensitive domains such as health, finance, and critical infrastructure.

Stakeholders noted that the deeper challenge is not simply aligning reporting channels, but harmonising the underlying regulatory philosophies. Risk-based cybersecurity (NIS 2), safety-based product regulation (CRA), and fundamental rights-based breach notification (GDPR) operate on different conceptual foundations. Consolidation requires reconciling these differences, not merely merging reporting portals.

Enforcement capacity and structural imbalances

Finally, enforcement capacity remains uneven across Member States. Smaller authorities face disproportionate burdens in supervising large, cross-border providers of digital infrastructure and cloud platforms. This creates systemic delays, inconsistent enforcement outcomes, and uneven implementation of cybersecurity obligations.

The problem is particularly acute in sectors where a small number of Member States host the majority of critical operators. Stakeholders stressed that without addressing enforcement capacity, even well-designed legislation will struggle to deliver timely and effective results².

Towards targeted structural improvements

The EU's cybersecurity framework does not appear to require wholesale redesign, but rather targeted structural improvements:

- consideration of cybersecurity from the ground up whenever new law is conceptualised;
- harmonisation of incident-reporting definitions, thresholds, timelines, and templates;
- consolidation of notification channels where politically feasible;
- clearer proportionality guidance across regimes;
- stronger accountability mechanisms for EU-level coordination bodies;
- clarification of interactions between NIS 2 and sectoral frameworks such as the EHDS; and
- support for enforcement capacity in smaller Member States.

These targeted reforms would help ensure that the EU's cybersecurity architecture becomes more coherent, proportionate, and operationally realistic, without undermining the EU's strategic ambition or the fundamental rights it seeks to protect.

² One participant argued, however, that maintenance of the NIS 2 main establishment principle is crucial for single market harmonisation.

8. THE BETTER REGULATION PROCESS: CREATING, EVALUATING, IMPROVING, AND SIMPLIFYING EU LAWS AND REGULATION

Key findings

The EU's regulatory ambition is substantially outpacing the ability of firms and Member States to implement the laws and regulations that are being enacted. The EU's better regulation process should be helping to ensure that the quality of laws remains high; however, it falls some short in some areas, even though it consistently ranks well in international assessments.

The EU's better regulation process comprises (i) *ex ante* impact assessment to ensure that legislative proposals are thought through carefully before they are submitted; (ii) *ex post* evaluation to periodically review whether the individual laws already in place are still relevant to the problems they were meant to address, are effective and efficient in addressing them, and are still consistent with the EU legislative *acquis*; (iii) flanking measures to periodically trim back bloat in the *acquis*; and (iv) supporting strategies and measures.

The European Commission, Parliament, and Council have agreed that better regulation is a joint responsibility, but in practice it is largely left to the Commission.

At present, about 60% of Commission proposals that go through the ordinary legislative procedure are accompanied by impact assessments; however, the Commission often neglects to submit impact assessments that should have been required. The omission tends to be based on unconvincing claims of urgency.

Public consultation is a key building block for proper impact assessment. The omnibus proposals frequently lacked proper consultations. When consultations are held, SMEs carry too little weight in them and EU independent agencies do not appear to weigh in as much as they could.

The impact assessment is supposed to take innovation into account along with impacts on SMEs, but these measures are often ineffective, last-minute box-ticking exercises.

The impact assessment corresponds to an assessment of a legislative measure as submitted by the Commission, not as enacted. The European Parliament and Council are under little pressure to refrain from adding 'feel good' provisions whose costs and impacts are not analysed until years later, if ever.

Given growing global uncertainty and geopolitical tensions, it is likely necessary to design future laws more for robustness across multiple scenarios than it was in the past.

Also, with an explosion in the number of digital laws, the need to look across policy silos has grown. The silo structure of the Commission makes this difficult; in addition, the Commission may lack specialised expertise.

There is very little pressure to do the *ex post* evaluation well, or for that matter, to do it at all.

Newer laws usually include a schedule for evaluation, and it is usually adhered to; in the past, it is likely that not as many evaluations were conducted as should have been.

The Commission's new focus on simplification and implementation is important and positive, but it is too soon to say whether it is effective.

The 'one in, one out' strategy needs rethinking – it seeks to optimise the wrong things.

The 'Think Small First' strategy is largely aspirational rather than operational. A general problem is that SMEs are often suppliers to larger firms; consequently, exemptions meant to reduce burdens on SMEs often have only limited practical effect.

Fragmentation of Member State law and regulation continues to be a burden for cross-border business. The SOLVIT network and the Single Digital Gateway (SDG) potentially represent important contributions to cross-border commerce and e-commerce, but they fall short of their potential.

The Task Force invested about a third of its time in assessing the better regulation process, rather than specific laws. One cannot hope to improve the sausage that is produced without improving the quality of the sausage factory that produces it.

The EU's better regulation process comprises four main elements:

- *ex ante* impact assessment to ensure that legislative proposals are thought through carefully before they are submitted;
- *ex post* evaluation to periodically review whether the individual laws already in place are still relevant to the problems they were meant to address, are effective and efficient in addressing them, and are still consistent with the EU legislative *acquis*;

- flanking measures to periodically trim back bloat in the *acquis* through processes such as the regulatory fitness and performance programme, REFIT; and
- supporting measures such as the SDG and the SOLVIT network to assist businesses and individuals in navigating the complexity of the system, especially as regards cross-border issues among the Member States.

International assessments, including those undertaken by the OECD, consistently ascribe high marks to the EU's better regulation process; this is, however, based on international comparisons that arguably set a low bar. Some insiders would contend that the overall quality of the process has declined a bit over the past decade. Be that as it may, it is clear that there is ample room for improvement.

An overarching issue is that better regulation is intended to be a joint responsibility of the European Commission, Parliament, and Council, but in practice is largely left to the Commission. Building on earlier agreements, in 2016 the three European institutions responsible for enacting good laws (Commission, Parliament, and Council) jointly signed an updated Interinstitutional Agreement to specify how they would cooperate (European Parliament, Council of the European Union, and European Commission, 2016). To date, this agreement remains largely aspirational – Parliament mainly relies on the Commission, and the Council does hardly anything at all to supply its end of better regulation. A three-legged stool cannot properly stand if two legs are unable to bear the load (see Figure 3).

Recommendation 9. The three co-legislators committed in 2016 to jointly implement the better regulation system. Parliament and the Council need to step up to do their share in order to provide better checks and balances within the overall better regulation system.

Figure 3. Conceptual illustration of the 2016 Interinstitutional Agreement as a three-legged stool: a progressively weakened Parliament and Council leave the framework unstable



Source: Generated by ChatGPT.

In this section, we consider the process used to generate *ex ante* impact assessments (Section 8.1), the process used for *ex post* evaluations (Section 8.2), and the various supporting measures in place (Section 8.3).

8.1. *EX ANTE* IMPACT ASSESSMENT

After more than 20 years of progressive refinement, the procedure for *ex ante* impact assessment, supported by the review of the Regulatory Scrutiny Board (RSB), often works reasonably well; nevertheless, there is ample room for improvement, both in the functioning of the impact assessment process and in its linkages to the rest of the better regulation framework.

According to Bucher & Golberg (2026a), about 60% of Commission proposals that go through the ordinary legislative procedure have been accompanied by impact assessments in recent years. Is that enough? A key threshold question is whether impact assessments are conducted in all of the instances where they should be. That is a rhetorical question: the answer is the Commission frequently neglects submitting impact assessments that should have been required. The Commission has had a long-standing tendency to skip the impact assessment for legislation that is politically challenging –

usually the very laws that would most benefit from careful assessment. In the past, the omission has often been based on unconvincing claims of urgency (Marcus, Midões, & Schout, 2019).

The issue is now coming to a head. The new omnibus legislative measures represent a major component of the Commission's focus on regulatory simplification, but not a single one was accompanied by an impact assessment, even though several of the omnibus legislative proposals put forward changes with far-reaching implications. As we explained in Sections 7.1 and 7.2, this led the European Ombudsperson to issue a finding of maladministration against the Commission, and also to harsh criticism in CEPS studies for the European Parliament (Marcus, 2026). The Ombudsperson called on the Commission not only to better justify any claims of urgency, but also to establish a clear procedure as to what steps may legitimately be skipped in true instances of urgency.

The Commission responded to the Ombudsperson's finding with a Communication in April 2026 (European Commission, 2026). A full review is well beyond the scope of this report, but we note that some experts have argued that it falls considerably short of what is needed (Bucher & Golberg, 2026b).

In addition to a substantial increase in the number of new laws, there is also a simply enormous number of delegated acts and implementing acts (see Section 2). These acts are rarely subject to an impact assessment. In some cases (not all), the changes put forward are complex enough that an impact assessment would have been warranted (Bucher & Golberg, 2026a).

Recommendation 10. The Commission should redouble its efforts to ensure that every legislative proposal is accompanied by an impact assessment document, except in cases of genuine urgency. If it is truly impractical to provide an impact assessment when the legislative proposal is submitted, the Commission should, if possible, follow up a few months later with an abbreviated impact assessment.

The impact assessment corresponds to an assessment of a legislative measure as submitted by the Commission, not as enacted. Parliament and the Council are under little pressure to refrain from adding 'feel good' provisions whose costs and impacts are not analysed until years later, if ever. The problem is well known – there is, for example, a proposal in the Letta report (2024) that the cost benefit analysis of an impact assessment should be constructed in a modular fashion, so as to enable updates as major changes are made in the course of the legislative process. Nonetheless, the problem persists, and no effort to correct it is visible (or possible as long as Parliament and the Council refuse

to shoulder their burdens under the Interinstitutional Agreement (European Parliament, Council and European Commission, 2016)).

The failure to update the impact assessment has knock-on effects. For instance, the *one in, one out* strategy seeks to reduce the burden of new laws in comparison with the burden estimated when they are proposed, because no one is in a position to estimate the burden of a new law as enacted. In other words, this deficiency means that *one in, one out* is seeking to reduce burden compared with a largely fictional number.

Recommendation 11. Any significant piece of EU legislation will ultimately differ substantially from the initial legislative proposal submitted by the Commission. Late in the process but prior to final enactment, an addendum to the impact assessment should be prepared to summarise the differences between the law as proposed and the law as enacted, including an update to the expected administrative costs and adaptation costs.

The public consultation process is a key input to the impact assessment. Over the years, the OECD has tended to give high marks to the Commission's public consultation process; still, Task Force participants were not convinced that public consultations were fully or properly taken into account in new legislative proposals in general.

As noted at several points in this report, the omnibus proposals whereby the Commission sought to improve and simplify Commission regulation in eight areas (sustainability, InvestEU, agriculture, small mid-caps and digitalisation, defence, digital, chemicals, and the environment) represent a particularly egregious and also ironic lapse. 'All were published after limited consultations and without an impact assessment for [alleged] reasons of emergency and political importance.' (Bucher & Golberg, 2026a) This issue comes up repeatedly in this report, including in Section 8.3.

Task Force participants questioned whether impact assessments paid enough attention to SMEs, and also to the EU's own independent agencies. This is partly a public consultation question, and partly a broader impact assessment question. The issue with SMEs is well known – they tend to be far less able than large enterprises to invest in responses to public consultations and other forms of advocacy. Public consultations are by nature biased to the extent that the respondents are *self-selected*. As a result, large enterprises tend to be far better able than SMEs to defend their interests. We return to this point in Section 8.3.

Task Force participants were deeply concerned over potential lack of coherence across different EU laws, including inconsistent definitions. The figures in Section 2 should make clear that this is not an idle concern – not only has there been a quadrupling in the

number of digital laws in the 12 years leading up to 2024, but also a doubling in their length over the past 20 years. Moreover, the number of potential pairwise interactions among 88 laws is close to 4 000 – well beyond what even highly skilled regulatory experts can hope to keep in their heads.

This concern is exacerbated by the silo structure of the Commission, and to some extent also of Parliament. There is only limited ability to look across the silos to identify potential mismatches prior to enactment (see Section 8.3).

Eventually, automated tools such as AI or even digital twins might be useful in identifying conflicts and inconsistencies. A few years ago, this might have seemed far-fetched, but rapid technological progress may be bringing us closer. In any case, we are not there yet.

Despite good intentions, Commission officials are not technology experts. Are they fully up to the job of designing the rules that are going to be needed in the years to come? Is there an increased need for internal training of Commission staff, or better integration of external expertise?

Relatedly, a participant worried that not enough consideration is given to the potential impact of proposed digital legislation on the technical infrastructure that underpins the global internet. With increasing calls for national control over digital environments, protecting the integrity of the core infrastructure that enables the internet is essential. Potential conflicts with existing technical standards, protocols, and cooperative frameworks should be avoided in order to protect the technical integrity of the internet and prevent its fragmentation or destabilisation.

Impact assessment under the better regulation process seeks to identify the best way forward under expected future conditions. There has always been some recognition of an uncertain future; however, the future has become far less predictable than it was even five years ago. We are now confronted with accelerating technological change, geopolitical disruption, and post-pandemic uncertainty. Is robustness of policy options across multiple scenarios more important than optimality under a single expected scenario? Are changes needed to impact assessment under the better regulation process to take greater account of optimising results, not only under an expected future, but also under a range of radically different futures? Do scenario analysis or foresight, for instance, need to play a greater role in legislative design going forward?

Finally, there was a general concern in the Task Force that implementation might not be given enough weight in the impact assessment. The Commission has taken a number of steps to strengthen the focus on implementation. We return to this point in Section 8.3.

8.2. *EX POST* EVALUATIONS

The *ex post* evaluation process appears to be challenged to a far greater extent than that for *ex ante* impact assessment. The reasoning is simple: there is very little pressure to do the evaluation well, or for that matter, to do it at all. For comparison, if the Commission fails to submit a proper impact assessment, it may get pushback from Parliament and the Council, and may face obstacles in getting its desired law enacted. But if it fails to submit an evaluation, or submits a euphemistic ‘nothing to see here’ evaluation, there are no consequences. Most likely, the dysfunction will not be noticed; even if it is noticed, no action will be taken as a result.

This pessimistic assessment parallels that of Bucher & Golberg (2026a):

Commission ex-post evaluations of legislation are weak, often ill-timed, of mixed quality and with questionable impact on further policy development. They lack evidence and relevant data and often have limited stakeholder input. The RSB scrutiny comes too late in the process to improve data collection or methodology. For amendments to existing legislation, the RSB has indicated that only up to a third of ex-post evaluations are of sufficient quality to inform the associated impact assessment.

As regards timing, it is important that evaluations are undertaken on an appropriate schedule; otherwise, mid-course corrections for new or existing laws will come too late. At the same time, there might be little value in an evaluation that is conducted too early, before the impacts of a new law are visible.

Recommendation 12. The *ex post* evaluation to which all significant programmes are in theory subject should in fact be carried out on a timely basis. Going forward, the impact assessment, and ultimately the legislation itself, should establish a default schedule for subsequent evaluation; however, this should be done in such a way that it does not preclude joint evaluation of multiple interrelated measures.

It is hard to be quantitatively definitive as to whether enough evaluations are being undertaken because the number of evaluations is tricky to measure. The relationship between laws and evaluations is not always one-to-one. Some evaluations address only a portion of a law; others simultaneously address more than one law, especially where a REFIT procedure is concerned.

Despite these limitations, many of the evaluations that have been conducted can be identified, so a very rough count is possible. Simply comparing the number of impact assessments to the total size of the EU legislative *acquis* suggests that far fewer

evaluations were conducted in the past than might have been expected. By contrast, for newer legislative measures, each law typically specifies a cycle for evaluation. The data that we collect for our dataset of EU laws (Zenner, Marcus, & Sekut, 2025) suggest that these schedules for newer laws are adhered to for the most part.

Even trickier is assessing whether an evaluation is well done, and properly and honestly reflects reality. Here, a structural problem rears its head. The Commission is responsible in practice for evaluations. It is also responsible for the initial formulation of all laws. There is an obvious incentive problem here – the Commission is not a neutral party. Most of the time, the Commission will not wish to document any errors that it made in formulating a law; in other cases, the Commission may have already decided that changes are needed. Either way, the evaluation report is likely to strongly reflect the Commission’s prior expectations.

Comprehensive evaluation reports often reflect outside expertise, but this does not solve the problem. Few consultants will have the courage to publish a report that contradicts the Commission’s prior assumptions, and there is no incentive for them to do so.

In any event, it is generally the Commission that writes the evaluation report, not the consultants. The report is nominally subject to review by the RSB; still, by the time the RSB sees the evaluation report, the damage has already been done. Options to correct a deficient report tend to be limited.

Those who teach do not permit their students to grade their own exams. There is a strong argument to be made that we will never get truly objective evaluations until responsibility for the evaluation is shifted to a truly neutral party.

A number of experts have suggested moving the *ex post* evaluation function to the Court of Auditors (Bucher & Golberg, 2026a; Marcus, 2024). Whether the Court of Auditors is the most appropriate entity, however, would require careful consideration.

Recommendation 13. The process of evaluating legislation *ex post* should not be done by the Commission. Moving the function to, for instance, the Court of Auditors, together with assigning it sufficient staff resources, could lead to more objective and impartial evaluations. Whether the Court of Auditors is the most appropriate entity, however, would require careful consideration.

The tendency in evaluation reports is to measure the effectiveness and efficiency of the various measures put in place by the law, without considering whether they actually contribute to solving the problems that motivated the creation of the law in the first place. This is perhaps understandable – it can be challenging to demonstrate the causal role of

the law in mitigating the underlying problem, or conversely to demonstrate that if the problem worsened, that the law nonetheless was (or was not) positive relative to the counterfactual. This is a classic ‘lamppost problem’ – we look for the lost coin under the lamppost because the light is better there, even though that is not where the coin was in fact lost.

Be that as it may, in the absence of outcome-oriented metrics that link the effects of the law to the initial problem definition and objectives, the evaluation study cannot be very meaningful.

Recommendation 14. In assessing the effectiveness of a law, the *ex post* evaluation must consider whether the law is actually mitigating the problem for which it was created. To make that possible, much more attention is needed when the impact assessment is drafted to ensure that data will be collected that enable proper subsequent evaluation.

8.3. SIMPLIFICATION OF THE OVERALL STOCK OF EU LAWS AND REGULATIONS

As we have seen in Section 2, the number of EU laws for the digital world has grown at an explosive pace. The practical consequence is that the EU’s regulatory ambition is substantially outpacing the ability of firms and Member States to implement the laws and regulations that are being enacted.

This has not gone unnoticed. A number of steps have been taken that seek to bring the overall EU legal and regulatory system into better alignment, as we explain in this section, but there is still much work to be done.

An overall focus on simplification and implementation

Largely as a response to the Draghi report (2024b), the Mission Letters from the Commission President to the Commissioners directs each of them to focus on regulatory simplification and implementation. Each Commissioner is to report back annually as to what they have accomplished, and these reports are then grouped together into an annual [Progress Report on Simplification, Implementation and Enforcement](#) by a new function within the Secretariat-General.

This is promising, and helps to set the right tone, but it is too soon to say whether it is effective. The first report was issued in October 2025 – too early into the current five-year mandate to judge effects. Aside from that, neither DG-specific nor overall KPI targets have been established, so there can be no crisp definition of success or failure.

Avoiding needless burden on innovation

Innovation and SME burdens are structurally linked: both arise from cumulative regulatory obligations, fragmented implementation, and the absence of impact assessment for Parliament and Council amendments.

Every Commission impact assessment is required to analyse effects on innovation, research ecosystems, data availability, and emerging technologies. The Better Regulation Guidelines call for assessing whether proposals enable experimentation, support new business models, and avoid unnecessary barriers to technological development. In principle, this should ensure that digital regulation is designed in a way that protects fundamental rights while preserving Europe's capacity to innovate. Yet in practice, innovation analysis remains one of the weakest components of the regulatory process.

A first structural problem is that impact assessments typically contain only brief statements noting that innovation may be affected, without modelling how regulatory obligations interact with R&I ecosystems, data flows, technology adoption, or technological development cycles. Quantitative analysis is rare, and the cumulative innovation effects across multiple digital instruments (e.g. the GDPR, DSA, DMA, Data Act, AI Act, EHDS, NIS 2, and CRA) on data access, documentation, cybersecurity, transparency, and risk management, are almost never assessed.

A second weakness is that innovation impacts are not systematically considered after a legislative proposal is submitted because, as previously noted, Parliament and Council amendments are not subject to mandatory impact assessment. This allows additional obligations, new rights, or expanded scope to be introduced without evaluating their effects on innovation.

A third challenge is failure to fully take into account the degree to which imposing limitations on data availability, such as new consent requirements, or creating uncertainty around pseudonymisation and anonymisation, impact innovation.

A fourth limitation is that innovation impacts are not monitored after adoption. The Better Regulation Guidelines foresee *ex post* evaluation and fitness checks, but these are infrequent and slow, and they rarely focus on innovation outcomes.

Taken together, these factors mean that innovation impacts are formally recognised but weakly operationalised.

Avoiding needless burden on SMEs (and mid-caps)

The interest in avoiding needless burden on SMEs is long-standing, but results to date have at best been mixed. The Think Small First principle has been an official component of the EU's regulatory thinking since 2008. It is embedded in the Better Regulation Guidelines, the SME Test, and the RSB's checklist. On paper, the principle is intended to ensure that legislation is designed from the perspective of smaller firms, with regulatory burdens minimised wherever possible and exemptions or simplified pathways considered systematically. But in practice, its impact on the design and implementation of digital regulation has been modest – it is aspirational, but poorly operationalised. Many of the challenges parallel those for guarding against burdens on innovation.

One constraint is that even though every Commission impact assessment is required to contain an SME section, these are frequently short, superficial, and added to the impact assessment as an afterthought at the last minute.

Another issue is that even when legislation exempts SMEs from its scope, the practical effect is often minimal because SMEs operate within supply chains dominated by larger firms. In practice, SMEs must meet the same requirements to remain suppliers. As a result, SME exemptions frequently fail to reduce real-world burden.

As with innovation measures, the Think Small First principle applies only to Commission proposals. Parliament and Council amendments are not subject to mandatory SME impact assessment. There is no back pressure against costly 'feel good' measures being added.

These factors mean that Think Small First continues to function more as a political signal than an operational constraint on regulatory design or implementation.

Reducing overall burden: the one in, one out principle

As with many of the other measures, the one in, one out principle is promising in practice, but poorly operationalised. Beyond that, it has weak conceptual underpinnings.

Contrary to what the casual reader might assume, 'one in, one out' does not mean that for each new law enacted, a different law must be repealed. What it actually means is that for each new law enacted, an equivalent amount of administrative burden must be alleviated elsewhere, ideally in burden on the same sector, with burden calculated according to the Commission's original impact assessment.

The problems with this approach should be obvious. First, it addresses only *administrative burden*, with no consideration of *implementation or operational burden*. Second, it is seeking to compensate for burden in the law as proposed, which may be very different

from administrative burden in the law as enacted. This is yet another casualty of the failure to reassess the cost of legislation as it undergoes major, potentially costly amendments.

Recommendation 15. The ‘one in, one out’ principle is genuinely important and promising but it needs to offset the administrative cost of a new law as enacted, not just the administrative cost of the law as initially proposed. One in, one out cannot hope to fully offset the adaptation costs of the law, which will usually be far greater than the administrative costs, but it should at least monitor the adaptation costs for comparative purposes. Ideally, the economic gains from the law should also be reflected.

Simplifying and consolidating groups of laws: looking across the silos

A key mechanism that could potentially be used to prune back regulatory excess is the *REFIT programme*. Under the REFIT programme, a *codification* seeks to achieve simplification by consolidating all of the provisions of an existing legal act and its amendments into a new legal act; a *recast* goes further by incorporating substantive amendments along with the consolidation.

In practice, very little of this kind of simplification has been done. It is hard work, and not necessarily politically rewarding for politicians or DGs. The first von der Leyen Commission prepared 17 recasts and 8 codifications, similar to the Juncker Commission, which proposed 22 recasts and 8 codifications. By comparison, the Barroso II Commission put forward only 2 codifications and 14 recasts. Compared with the roughly 400 new laws that were proposed in each of these five-year legislative terms, this is very little.

This process could be important because REFIT is one of the few simplification processes that ‘looks across the silos’. Most EU simplification tools are driven by a single Commission DG and look at a single law; however, the impact of the increasing volume and complexity of EU law (especially digital law) is to a significant degree cumulative. A more holistic approach is needed.

Recommendation 16. The Commission should be making greater use of the REFIT process to simplify existing laws so as to reduce needless regulatory complexity.

The omnibus regulations potentially look across the silos, but the omnibus measures implemented to date have been rushed jobs. As noted at multiple points in this report, they suffer from a failure to conduct proper, unbiased consultations, and a failure to

conduct impact assessments when they are needed. They have sought to introduce far-reaching structural changes (e.g. redefining personal data) without evidence, and potentially generated cross-instrument inconsistencies. In their present form, they fall short.

Recommendation 17. The omnibus process could be valuable, but its effectiveness has been limited to date by process deficiencies in how it has been implemented. Simplification is by no means simple. Proper consultation and analysis are needed. Where changes with complex implications are put forward, the Commission must conduct a proper impact assessment. Purported urgency is not an excuse.

Task Force participants discussed the possible need for institutional change at the EU level to address these cross-silo issues, including in particular the lack of coordination across Commission DGs.

One possible approach that was discussed would be to create a new single market agency modelled on the Body of European Regulators for Electronic Communications, the European Banking Authority, or European Securities and Markets Authority, drawing on seconded national expertise. This idea seems promising, but it needs further development to clarify the role and authority of such an agency.

Commission functions are not the only instances of silos within the Commission. The Task Force also briefly considered fragmentation among Commission IT systems. Successive legislative acts have mandated new portals and tracking systems without any overarching plan for IT architecture, yielding hundreds of parallel systems with limited coherence.

On a different note, Task Force participants debated whether the regulatory simplification process has become too bureaucratic.

8.4. SINGLE MARKET ASPECTS OF SIMPLIFICATION AND IMPLEMENTATION

Some measures seek to avoid or reduce fragmentation; others seek to deal with the consequences of fragmentation.

Reducing fragmentation across the Member States

The Task Force discussed at length how to avoid excessive legislative volume, complexity, and inconsistency in design, how to reduce gold-plating during transposition, and how to mitigate practical implementation gaps in some Member States. Some of these are more easily addressed than others.

As far as reducing the volume of legislation, the simplest way would be to enact less of it! This is easier said than done, first because many new challenges have emerged in recent years, and second because one cannot reduce complexity in current legislation without introducing new legislation to fix the old, thereby potentially also generating new dilemmas.

For reducing transposition issues and fragmentation, the European institutions are progressively enacting more and more regulations and fewer directives. Regulations do not require transposition (except in the three EEA countries), and they leave much less room for creative Member State interpretation. Relatedly, measures could explicitly call for *maximum harmonisation*, which is only rarely used today.

A mix of approaches would likely be needed to reduce gaps. Increasing capacity in the Member States is clearly an element, both through more staff and probably also through better training. This has cost implications.

At the same time, the goal cannot be total EU-wide uniformity of implementation – what is needed instead is a better and more appropriate balance between centralisation and decentralisation of implementation within the EU. Centralisation tends to offer economies of scale and scope; decentralisation is better suited to accommodating local needs and preferences, as is recognised in the EU principle of *subsidiarity*. There is no single, universally correct solution (Oates, 1972).

Recommendation 18. Reducing fragmentation requires a mix of measures that strengthen consistency in implementation and improve the practical functioning of the single market, while still recognising that decentralised implementation has its place. The EU should make greater use of regulations and explicit maximum harmonisation clauses to limit divergent national interpretations; reinforce Member State implementation capacity through targeted funding, training, and technical assistance; and ensure that guidance, templates, and standardised procedures are available early enough to reduce the risk of inconsistent national approaches. These steps would not eliminate fragmentation entirely, but they would materially reduce the gaps that currently arise from uneven administrative capacity, gold-plating, and divergent enforcement practices across the Member States.

The SOLVIT network

When firms encounter obstacles to the free movement of goods (for instance, a failure of Member State authorities to adhere to the principle of *mutual recognition*), they can turn to SOLVIT, an informal problem-solving network. SOLVIT's aim is to remove unjustified obstacles to free movement via informal means of dialogue and cooperation between the

SOLVIT centres in the respective Member States, thus avoiding more complex and lengthier formal, legal procedures.

SOLVIT seems to work reasonably well in helping consumers to deal with problems related to recognition of professional qualifications; however, it seems to be underperforming as regards helping e-merchants to deal with cross-border problems. Businesses rarely use it. A Eurochambres survey found that if e-merchants encounter a single market problem, they are far more likely to hire a lawyer (35.0% very likely, 41.5% likely), or to simply give up (9.5% very likely, 23.3% likely), than to rely on the SOLVIT network (4.2% very likely, 19.3% likely) (Eurochambres, 2024, p. 9; Marcus, 2024b). E-merchants presumably judge SOLVIT as being too great an effort, or the prospects of success as being too small, or both.

There are probably multiple explanations for this lack of effectiveness, starting with insufficient staffing in some Member States. Merchants seem not to be aware of its existence. It can only be brought to bear when a problem has already emerged, and if so, it addresses the specific instance rather than the underlying structural problem. And SOLVIT lacks enforcement power.

Recommendation 19. The SOLVIT network should be strengthened and modernised so that it becomes a genuinely useful tool for cross-border merchants rather than a little-known mechanism used mainly by individuals. This requires linking SOLVIT with business-facing ecosystems (chambers of commerce, enterprise agencies, and sectoral associations), and improving staffing and expertise in national centres – especially for digital-regulation cases. It also involves creating a clearer escalation pathway so that unresolved or systemic problems feed into infringement-prevention mechanisms and the Commission’s annual Progress Report on Simplification and Implementation. Greater visibility, minimum capacity standards, and a structured feedback loop would materially increase SOLVIT’s credibility and make it a more effective instrument for addressing the practical single market barriers faced by merchants.

The Single Digital Gateway

The SDG is a seemingly promising programme that likewise seems to be underperforming in practice. The SDG seeks to ensure that people and merchants have access to reliable information about laws and regulations in all of the Member States in commonly spoken languages, primarily English. Although the SDG has compiled a large volume of information, and it is being accessed millions of times per year, it does not appear to be accessed as often as it potentially could be. In a recent Eurochambres survey of 1 004

business owners and entrepreneurs across all EU Member States from September to November 2023, 61.2% identified ‘inaccessibility to information on rules and requirements’ as either a significant or an extremely significant single market impediment (Eurochambres, 2024, p. 4). This cannot be viewed as a solved problem.

Once again, there are likely multiple reasons. As with SOLVIT, merchants seem not to be aware of its existence. For that matter, policymakers do not seem to be aware of its existence. SDG documents are not readily discoverable via standard search engines. The quality of documents provided varies across the Member States. More fundamental is that the SDG is a document repository, but the business users who could potentially profit from the SDG probably need more advisory or consultative services – a likely opportunity for the use of AI, subject to suitable safeguards against hallucinations and other risks.

Recommendation 20. The Single Digital Gateway should evolve from a document repository into a genuinely usable compliance tool for cross-border merchants. To achieve this, SDG content must become easily discoverable through search engines, supported by structured metadata and minimum quality standards across Member States. Merchants should encounter clear summaries, step-by-step compliance pathways, and alerts for regulatory changes rather than raw documents alone. The SDG should also be linked to sector-specific portals and business-onboarding tools, and enhanced with advisory functionality – potentially including carefully safeguarded AI assistance – to help users identify relevant obligations quickly and reliably. These measures would significantly increase the SDG’s visibility, usability, and practical value for businesses operating in the single market.

REFERENCES

- Aboy, M., Minssen, T., & Vayena, E. (2024), '[Navigating the EU AI Act: implications for regulated digital medical products](#)', *npj Digital Medicine* 7, 237.
- Ahern, D. (2025), '[Operationalising AI regulatory sandboxes under the EU AI Act: the triple challenge of capacity, coordination and attractiveness to providers](#)', *Cambridge Forum on AI: Law and Governance* 1, e35.
- AI Act Blog (2026), '[Digital Omnibus & AI Act: what changes for compliance](#)', Praxikon (formerly aiactblog.nl).
- Bagonza, J.K. (2026), '[Regulating Platform Content Governance at Scale under the EU Digital Services Act \(DSA\) and the DSA Transparency Database](#)', *World Journal of Advanced Research and Reviews* 30(2), 2684-2695.
- Bang, J. (2026), '[Regulatory Governance of AI in the Generative AI Era: A Comparative Study of South Korea's AI Basic Act and the EU AI Act for Sustainable Digital Transformation](#)', *Laws* 15(3), 42.
- Bostoen, F., & Monti, G. (2025), '[The rhyme and reason of gatekeeper designation under the Digital Markets Act](#)', *Journal of Antitrust Enforcement*, jnae054.
- Botta, M. (2026), '[Digital Markets Act: two years after, where do we stand? Some reflections on DMA achievements and future challenges](#)', *Journal of Antitrust Enforcement* 14(2), 386-393.
- Broadbent, M. (2021), '[Implications of the Digital Markets Act for Transatlantic Cooperation](#)', Center for Strategic and International Studies.
- Bruegel (2025), '[The case for a European Union digital enforcement authority](#)', Bruegel Policy Brief.
- Bucher, A., & Golberg, E. (2026a), '[Better regulation in the European Union needs a fresh start](#)', Bruegel.
- Bucher, A., & Golberg, E. (2026b), '[The European Commission's recommitment to better regulation is yet to be proven](#)', Bruegel.
- Center for Strategic and International Studies (2026a), '[The New Containment Doctrine: How the United States Is Using Trade to Stop Digital Regulation](#)', CSIS.
- Centre for Future Generations (2026), '[Enforcement Spotlight: Spring 2026](#)', Centre for Future Generations.
- Chirita, A.D. (2022), '[Data-Driven Unfair Competition in Digital Markets](#)', Durham Law School Research Paper, SSRN.
- Council of the European Union (2026), '[Artificial intelligence: Council and Parliament agree to simplify and streamline rules](#)', press release, 7 May 2026.
- Cr  mer, J., Crawford, G.S., Dinielli, D., Fletcher, A., Heidhues, P., Schnitzer, M., & Scott Morton, F.M. (2023), '[Fairness and contestability in the Digital Markets Act](#)', *Yale Journal on Regulation* 40, 973-1011.
- Cr  mer, J., de Montjoye, Y.-A., & Schweitzer, H. (2019), '[Competition Policy for the Digital Era](#)', European Commission.
- Cr  mer, J., Dinielli, D., Heidhues, P., Kimmelman, G., Monti, G., Podszun, R., Schnitzer, M., Scott Morton, F., & de Streel, A. (2023), '[Enforcing the Digital Markets Act: institutional choices, compliance, and antitrust](#)', *Journal of Antitrust Enforcement* 11(3), 315-349.

- Darius, P., Breuer, J., Kruschinski, S., Loecherbach, F., Riedl, J., & Stier, S. (2026), '[Election research in the age of regulated data access under the EU Digital Services Act](#)', *Internet Policy Review* 15(1).
- de Elizalde, F. (2025), '[Fragmenting Consumer Law Through Data Protection and Digital Market Regulations: The DMA, the DSA, the GDPR, and EU Consumer Law](#)', *Journal of Consumer Policy* 48(3), 355-389.
- Digital Competition (2025), '[The Limits and Promises of the Digital Markets Act Review](#)', Digital Competition (archived copy).
- Dignum, V., Carli, R., & Titareva, T. (2026), '[Rethinking the Digital Omnibus' Impact on the EU AI Act: Simplification or Dilution?](#)', AI Policy Exchange Forum, AI Policy Lab, Umeå University.
- Drage, E., Pi, Y., Hollanek, T., Peters, D., & Yakar, S. (2025), '[The EU AI act in development practice: a pro-justice approach](#)', *AI and Ethics* 6(1), 6.
- Draghi, M. (2024a), '[Speech by Mario Draghi](#)', La Hulpe, 16 April.
- Draghi, M. (2024b), '[The Future of European Competitiveness: A Strategy for Europe](#)', Part A, Publications Office of the European Union.
- Ebers, M. (2024), '[Truly Risk-based Regulation of Artificial Intelligence: How to Implement the EU's AI Act](#)', *European Journal of Risk Regulation* 16(2), 684-703.
- Eder, N. (2024), '[Making Systemic Risk Assessments Work: How the DSA Creates a Virtuous Loop to Address the Societal Harms of Content Moderation](#)', *German Law Journal* 25(7), 1197-1218.
- Etteldorf, C. (2022), '[DMA: Digital Markets Act or Data Markets Act?](#)', *European Data Protection Law Review* 8(2), 255-261.
- Eurochambres (2024), *2024 Eurochambres Single Market Survey: Overcoming obstacles, developing solutions*.
- European Commission (2025a), '[Commission Delegated Regulation \(EU\) 2025/2050 of 1 July 2025 supplementing Regulation \(EU\) 2022/2065 by laying down the technical conditions and procedures under which providers of very large online platforms and of very large online search engines are to share data with vetted researchers](#)', OJ L 2025/2050, 9 October 2025.
- European Commission (2025b), '[The General-Purpose AI Code of Practice](#)', 10 July 2025.
- European Commission (2026a), '[Regulatory framework for AI](#)', European Commission.
- European Commission (2026b), '[Proposal for a Regulation amending Regulations \(EU\) 2024/1689 and \(EU\) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence \(Digital Omnibus on AI\)](#)', COM(2025) 836, 19 November 2025.
- European Commission (2026c), '[Commission decides to refer Czechia, Spain, Cyprus, Poland and Portugal to the Court of Justice of the European Union due to lack of effective implementation of the Digital Services Act](#)', press release IP/25/1081, 7 May 2025.
- European Commission (2026d), '[Report from the Commission to the European Parliament and the Council on the review of Regulation \(EU\) 2022/1925 \(Digital Markets Act\)](#)', COM(2026) 178 final, 28 April 2026.
- European Commission (2026e), '[The Digital Services Act](#)', European Commission.
- European Commission (2026f), *A Simpler, Clearer and Better Enforced EU Rulebook*.

- European Data Protection Board (EDPB) (2021), *Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities*.
- European Law Blog (2023), [Digital Services Coordinators and other competent authorities in the Digital Services Act: streamlined enforcement coordination lost?](#), European Law Blog.
- European Parliament, Council of the European Union, and European Commission (2016), *Interinstitutional Agreement on Better Law-Making*, European Union.
- Farrell, J., & Emborg, T. (2025), [An Introduction to the Code of Practice for General-Purpose AI](#), EU Artificial Intelligence Act, 14 August 2025.
- Fernández-Llorca, D., Gómez, E., Sánchez, I., & Mazzini, G. (2024), [‘An interdisciplinary account of the terminological choices by EU policymakers ahead of the final agreement on the AI Act: AI system, general purpose AI system, foundation model, and generative AI’](#), *Artificial Intelligence and Law* 33(4), 875-888.
- Freshfields (2026), [DSA decoded #10: Algorithmic transparency under the DSA](#), Freshfields Technology Quotient.
- Gartner, M. (2025), [‘The Digital Omnibus on AI: First Analysis of the EU’s Policy Pivot on the AI Act’](#), *Journal of AI Law and Regulation* 2(4), 376-383.
- Genicot, N., & Moraes, T. (2026), ‘Exploring the boundaries of AI regulatory sandboxes under the AI Act: flexibility and real-world testing’, *Cambridge Forum on AI: Law and Governance*.
- German Marshall Fund of the United States (2025), [The EU’s Digital Markets Act and Digital Services Act](#), GMF.
- Goanta, C., Zannettou, S., Kaushal, R., van de Kerkhof, J., Bertaglia, T., Annabell, T., Gui, H., Spanakis, G., & Iamnitich, A. (2025), [The Great Data Standoff: Researchers vs. Platforms Under the Digital Services Act](#), arXiv 2505.01122.
- Greser, J. (2024), [‘Access to data for academic purposes under the Digital Services Act’](#), *Przegląd Europejski* 4/2024.
- Gstrein, O.J., Haleem, N., & Zwitter, A. (2024), [‘General-purpose AI regulation and the European Union AI Act’](#), *Internet Policy Review* 13(3).
- Hacker, P., Cordes, J., & Rochon, J. (2023), [Regulating Gatekeeper AI and Data: Transparency, Access, and Fairness under the DMA, the GDPR, and beyond](#), SSRN working paper.
- Hogan Lovells (2025), [Who gets to see inside? The EU’s operational rules on data access under Article 40 of the DSA](#), Hogan Lovells.
- Hornkohl, L. (2024), [Collective Actions for Competition Law Violations and DMA Infringements Following the Transposition of the Representative Action Directive in Germany](#), SSRN working paper.
- Humpe, C., Barbu-O’Connor, C., Dowell, G., & Botas-Armero, R. (2024), [‘Unpacking the Digital Markets Act: a milestone ruling against ByteDance and its implications for potential gatekeepers’](#), *Competition Law Journal* 23(2), 104-112.
- Ibáñez Colomo, P. (2025), [‘Implementing the Digital Markets Act’](#), *Journal of European Competition Law & Practice*, Ipag010.
- Industry Associations (2025), [Industry Coalition Calls for Withdrawal of AI Liability Directive to Avoid Further Legal Uncertainty and Support Europe’s Competitiveness](#).

- Industry Associations (2026), [*Joint Industry Statement: EU Member States and Policymakers Must Not Undermine the Ambition of the EU Digital Omnibus*](#).
- International Center for Law and Economics (2025), [*ICLE Response to First Review of the Digital Markets Act*](#), ICLE.
- Istituto Affari Internazionali (2026), [*Making Enforcement Negotiable? The Digital Markets Act under US Pressure*](#), IAI.
- Jafarguliyev, A. (2025), [*Tying and Bundling in Digital Markets under the European Union Competition Law and Digital Markets Act*](#), SSRN working paper.
- Jones Day (2025), [*EU AI Act: European Commission Publishes General-Purpose AI Code of Practice*](#), Jones Day, August 2025.
- Justo-Hanani, R. (2025), '[*Risk-based approach to EU AI Act: benefits and challenges of co-regulation*](#)', *Policy Design and Practice* 9(2), 171-180.
- Keller, D. (2025), [*Delegated Regulation on Data Access Provided for in the Digital Services Act*](#), Stanford Public Law Working Paper, SSRN.
- Kilian, R., Jäck, L., & Ebel, D. (2025), '[*European AI standards: technical standardisation and implementation challenges under the EU AI Act*](#)', *European Journal of Risk Regulation* 16(3), 1038-1062.
- Kim, S.Y., & Ko, M.C. (2026), '[*Risk Management in AI Regulation: Comparative Insights from the EU AI Act and Korea's AI Basic Act*](#)', *Crisis and Emergency Management: Theory and Praxis* 16(1), 17-27.
- Koenig, C. (2025), '[*Germany's Gatekeeper Competition Law and Its Relationship with the Digital Markets Act*](#)', *European Competition and Regulatory Law Review* 9(3), 267-271.
- Kontosis, N., & Davalas, A. (2026), '[*Governing the Foundation: An Examination of the AI Act's New Rules for General-Purpose AI Models \(GPAI\)*](#)', *International Journal of Social Science and Economic Research* 11(2), 79-108.
- KPMG (2025), *A benchmark analysis of the Digital Markets Act Audit & Compliance Reports*, KPMG.
- Kusche, I. (2024), '[*Possible harms of artificial intelligence and the EU AI Act: fundamental rights and risk*](#)', *Journal of Risk Research*.
- Lee, B. (2024), '[*The EU Digital Markets Act Focusing on its Objectives, Principles and Approach*](#)', *Commercial Law Review* 43(2), 499-547.
- Leerssen, P. (2023), '[*An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation*](#)', *Computer Law & Security Review* 48, 105790.
- Leslie, W., O'Reilly, E., Lypalo, D., & Khodjamirian, S. (2025), '[*Same, same but different? Defining gatekeepers under the Digital Markets Act*](#)', *Journal of European Competition Law & Practice* 16(7), 401-410.
- Letta, E. (2024), [*Much More than a Market: Speed, Security, Solidarity*](#), European Commission.
- Liesenfeld, A. (2024), '[*The Legal Significance of Independent Research based on Article 40 DSA for the Management of Systemic Risks in the Digital Services Act*](#)', *European Journal of Risk Regulation* 16(1), 184-196.
- Ma, Z. (2026), '[*Evolving Beyond the Brussels Effect: EU Digital Diplomacy and the Broadening of External Digital Strategy*](#)', *Global Policy* 17(3), 475-486.

- Marcus, J.S. (2024a), [How to achieve better EU laws](#), CEPS.
- Marcus, J.S. (2024b), [Digital aspects of the EU Single Market: Still a work in progress?](#), CEPS.
- Marcus, J.S. (2026), [The European Commission is neglecting evidence-based law-making](#), CEPS.
- Marcus, J.S., & Rossi, M. (2024), [Strengthening EU digital competitiveness. Stoking the engine](#), EUI/RSC Centre for a Digital Society.
- Marcus, J.S., & Thomadakis, A. (2025), [Reporting Obligations](#), European Parliament, JURI Committee.
- Marcus, J.S., Midões, C., & Schout, A. (2019), 'To the commissioner responsible for Better Regulation', in Wolff, G.B., & Demertzis, M. (eds), [Braver, Greener, Fairer: Memos to the EU leadership 2019-2024](#), Bruegel.
- Marcus, J.S., Rossi, M., Mazzoni, L., & Parcu, P. (2025), [The impact of EU online platform regulation on EU productivity: A preliminary assessment](#), EUI/RSC Centre for a Digital Society.
- Mattioli, P. (2025), [Navigating the Complexities of the DSA's Enforcement Framework: Sincere Cooperation in Action?](#), *Utrecht Law Review* 21(1), 19-35.
- McIntyre, R. (2023), [Decentralisation and Recentralisation: An Institutional Analysis of EU Competition Law and the Digital Markets Act](#), *LSE Law Review* 8(3), 227-285.
- Montag, C., & Finck, M. (2024), [Successful implementation of the EU AI Act requires interdisciplinary efforts](#), *Nature Machine Intelligence* 6.
- Monti, M. (2024), [The Unity of Opposites in the Regulation of Social Media Platforms: Content Moderation Between the EU Digital Services Act and the US First Amendment Theories](#), SSRN working paper.
- Moravcová, D. (2023), [Impact of the DSA Regulation on Very Large Online Platforms](#), *Central European Journal of Comparative Law* 4(2), 163-176.
- Morrison & Foerster (2025), [EU Digital Omnibus on AI: What Is in It and What Is Not?](#), Morrison & Foerster, 1 December 2025.
- Nannini, L. (2025), [From categorical to contextual: interpreting high-risk classification for profiling-based AI recommender systems in the EU AI Act](#), *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* 8(2), 1836-1847.
- Novelli, C., Hacker, P., McDougall, S., Morley, J., Rotolo, A., & Floridi, L. (2026), [Getting regulatory sandboxes right: design and governance under the AI Act](#), *European Journal of Risk Regulation*.
- Novelli, C., Hacker, P., Morley, J., Trondal, J., & Floridi, L. (2024), [A robust governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities](#), *European Journal of Risk Regulation*.
- Oates, W. (1972), [Fiscal Federalism](#), Edward Elgar Publishing.
- Ohme, J., & Seiling, L. (2026), [Finally, access: how Article 40 DSA changes platform research in practice](#), *Political Communication* 43(4).
- Ortolani, P. (2022), [If you build it, they will come: the DSA's 'procedure before substance' approach](#), *Verfassungsblog*, 7 November 2022.
- Ortolani, P. (2023), [The Digital Services Act, Content Moderation and Dispute Resolution](#), SSRN working paper.

- Parisini, E., & Dervishaj, E. (2025), '[Emerging models of national competent authorities under the EU AI Act](#)', *Proceedings of the Conference on Digital Government Research (dg.o 2025)* TU Delft OPEN Publishing.
- The Platform Law Blog (2025), '[The Dawn of DSA Enforcement: Lessons from the Digital Services Coordinators' First Annual Reports](#)', The Platform Law Blog, 6 October 2025.
- Podszun, R. (2021), '[Private enforcement and gatekeeper regulation: strengthening the rights of private parties in the Digital Markets Act](#)', *Journal of European Competition Law & Practice* 13(3), 254.
- Popović, D.V., & Vujičić, N. (2026), '[Algorithmic Discrimination and the EU AI Act: Evaluating the Risk-Based Approach](#)', in Vujadinović, D., Kristoffersson, E., & Evola, M. (eds), *Law and Gender from an Intersectionality and Diversity Perspective*, Springer, 163-187.
- Pošćić, A. (2024), '[The Digital Markets Act: ensuring more contestability and openness in the European digital market](#)', *InterEULawEast* 11(1).
- Ramos, S., & Pianese, F. (2026), '[Regulating transparency: a critique of the "free and open source AI" definition in the EU AI act](#)', *AI and Ethics* 6(3).
- Revolidis, I. (2025), '[Regulating General Purpose Artificial Intelligence \(GPAI\) within the EU AI Act: Challenges and Considerations](#)', SSRN working paper.
- Sekut, K., & Marcus, J.S. (2024), '[Simplifying EU law: a cumbersome task with mixed results](#)', Bruegel.
- Sekwenz, M.-T., et al. (2026), '[Disarranged Harmonization of Transparency Reporting by Social Media Platforms under the Digital Services Act](#)', arXiv 2605.17655.
- Simone, C., & Laudando, A. (2025), '[Principles and obligations of the Digital Markets Act in regulating the economic power of gatekeepers: positive, negative or trade-off effects?](#)', *Electronic Markets* 35(1).
- Smith, J. (2025), '[Requiem for the EU: The Internal Costs of the Brussels Effect and the Digital Services Act as Case Study](#)', SSRN working paper.
- Tech Policy Press (2026a), '[What the EU AI Omnibus Deal Changes for the AI Act and What Lies Ahead](#)', Tech Policy Press (L. Caroli), 8 May 2026.
- Tech Policy Press (2026b), '[What the EU's First Digital Markets Act Review Actually Changes](#)', Tech Policy Press (M. Kirkwood), 30 April 2026.
- Värri, A. (2025), '[Harmonised standards to the AI Act: for medical devices, too](#)', *Finnish Journal of eHealth and eWelfare* 17(2).
- Vezzoso, S. (2024), '["Super-apps" and the Digital Markets Act](#)', *Journal of Antitrust Enforcement* 12(2), 331-337.
- Wei, J.T.-Z., Zufall, F., & Jia, R. (2024), '[Operationalizing content moderation "accuracy" in the Digital Services Act](#)', *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* 7(1), 1527-1538.
- Yasar, A.G., et al. (2024), '[AI and the EU Digital Markets Act: Addressing the Risks of Bigness in Generative AI](#)', arXiv 2308.02033.
- Yurukova, M. (2025), '[The role of the member states' digital services coordinator for ensuring coordinated and consistent enforcement of the Digital Services Act](#)', *Papers from the International Scientific Conference of the European Studies Department, Sofia University 'St. Kliment Ohridski'* 10, 176-187.

- Zenner, K., Marcus, J.S., & Sekut, K. (2024), [A dataset on EU legislation for the digital world](#), Bruegel.
- Zenner, K., Marcus, J.S., & Sekut, K. (2025), [Overview of EU legislation in the digital sector](#), CEPS.
- Zhong, H., O'Neill, E., & Hoffmann, J.A. (2024), '[Regulating AI: applying insights from behavioural economics and psychology to the application of Article 5 of the EU AI Act](#)', *Proceedings of the AAAI Conference on Artificial Intelligence* 38(18), 20001-20009.
- Zhybak, A.A. (2024), '[The gatekeepers compliance principles of the Digital Markets Act \(DMA\) as a guarantee of ensuring the rights of users of online platform services](#)', *Aktualni problemy derzhavy i prava* 101, 59-65.

APPENDIX A. TASK FORCE PARTICIPANTS

CHAIR

J. Scott Marcus, Associate Senior Research Fellow, CEPS

RAPPORTEURS

J. Scott Marcus, Associate Senior Research Fellow, CEPS

Artur Bogucki, Associate Researcher, CEPS

Jacob Griffith, Research Assistant, CEPS

INSTITUTIONAL OBSERVERS AND MEMBERS

Eline Chivot, Policy Analyst – Country Coordinator, DG Connect, European Commission

Sandra Leenders, EU Adviser, Digital Affairs, Dutch House of Representatives

Mariusz Maciejewski, Research Administrator, European Parliament

Noelia Martínez Huerga, International Project Officer in the Digital Sector Promotion Area, Secretariat for Digital Policies of the Government of Catalonia

Carla Perucca Iannitelli, Policy Adviser, Delegation of the Government of Catalonia to the European Union

PRIVATE SECTOR AND INDUSTRY MEMBERS

Andreas Aktoudianakis, Public Affairs EU Lead, Google

Cecilia Alvarez, EMEA Privacy Policy Director, Meta

Boniface de Champris, AI Policy Lead, CCIA Europe

Claudia La Donna, CEO, Edelman Brussels and Chair, EMEA Telecom, Media & Technology

Susanna Di Felicianantonio, Director, Global Public Affairs, KPMG International Ltd

Daniel Friedlaender, Senior Vice President & Head of Office, CCIA Europe

Sabine Gerdon, Public Policy, Amazon Web Services

Caroline Greer, Director of Public Policy & Government Relations, TikTok

Pierre Hausemer, Partner for the EU institutions, EY

Lorelien Hoet, Government Affairs Director EU, Microsoft

Thibault Larger, Head of academic engagement and partnerships, economic policy, International Public Policy, Amazon

Isabella Martorina, Business Development Leader for the EU Institutions, EY

Dijana Spasojevic, Director, EU and International Organisations, KPMG

Bartlomiej Telejko, Head of EU Data Governance, Google

Alessandro Zamboni, Managing Director & Partner, Wavestone Luxembourg

THINK TANK, ACADEMIC AND NGO MEMBERS

Dimitri Corpakis, Independent expert, Senior Research Fellow, SEERC, Fellow, Regional Studies Association, and former senior EU official

Maeva Devoto, Operations Coordinator, Government and IGO Engagement, ICANN

Jakub Kaczmarek, EU Regulatory Affairs Expert, Allegro

Chris Mondini, Vice President, Stakeholder Engagement, Europe and Managing Director for Europe, ICANN

Friederike Schueuer, Head of EU and Global AI Governance, Ada Lovelace Institute

Julia Smakman, Senior Researcher, Law & Policy, Ada Lovelace Institute

GUEST SPEAKERS

Luca Aguzzoni, Deputy Head of Unit, DMA team, DG CNECT, European Commission

Marco Botta, Part-time Professor at the European University Institute and Deputy Director, Centre for a Digital Society

Anne Bucher, Non-resident Fellow, Bruegel

Alexandra Lillo Campoy, Senior Specialist in Ethical Governance and AI Regulation, Observatory for Ethics in Artificial Intelligence of Catalonia (OEIAC)

Raquel Jorge Ricart, Associate Research Fellow, CEPS

Chiara Manfredini, Legal and Policy Officer, BEUC

Zach Meyers, Director of Research, CERRE

Franck Noël, Director, Access to and Reuse of Public Information at the EU Publications Office, European Commission

Lorenzo Pupillo, Associate Senior Research Fellow and Head of the Cybersecurity@CEPS Initiative, CEPS

Andrea Renda, Director of Research, CEPS

Alexandre de Streel, Academic Director, CERRE and Professor at Université de Namur

Kai Zenner, Head of Office and Digital Policy Adviser for MEP Axel Voss, European Parliament

APPENDIX B. PRINCIPLES AND GUIDELINES FOR THE TASK FORCE

The Task Force process is one of structured dialogue among experts, (former) politicians, diplomats, policymakers, representatives from industry, NGOs, academia and/or think tanks who are brought together for several meetings.

Participants

- The chair steers the dialogue during the meetings and advises CEPS as to the general conduct of the activities of the Task Force.
- Members of the Task Force provide input as independent experts.
- Rapporteurs are CEPS researchers who organise the meetings, conduct independent research, and draft the final report.

Objectives

- Task Force reports are meant to contribute to policy debates by presenting a balanced set of arguments, based on available data, literature and views.
- The reports seek to provide readers with a constructive basis for discussion. They do not seek to advance a single position or misrepresent the complexity of any subject matter.
- Task Force reports also fulfil an educational purpose and are drafted in a manner that is easy to understand, without jargon, and with any technical terminology fully defined.

Report

- Task Force reports reflect the views of the members.
- However, there does not need to be consensus or broad agreement among Task Force members for every recommendation that features in the report. Recommendations that triggered significant dissent are marked accordingly.
- Task Force reports feature data that are considered both relevant and accurate by the rapporteurs. After consultation with other Task Force members, the rapporteurs may decide either to exclude data or to mention these concerns in the main body of the text.



Centre for European Policy Studies
Place du Congrès 1
1000-B Brussels
Belgium