European Law Blog, 2026 · ISSN 2950-1970
Published: 21 October 2026
COMPETITION LAW

Collective compliance at the expense of competitive uncertainty?

Olga Kokoulina
University of Copenhagen

For decades, some of the most consistently exciting factual descriptions in competition law have come from cases on anticompetitive agreements covered by Article 101 of the TFEU: combinations of undertakings one would hardly imagine meeting around the same table, sudden price increases by identical percentages, hotel room reservations for regular meetings, handwritten notes and memoranda. At the core of these arrangements are prices and anticipated price increases, sales volumes and market shares, as well as a wide range of "price-setting factors" and pre-pricing communications offering intelligence about prospective quotation prices and trends (e.g. *C-286/13 P Dole Food and Dole Fresh Fruit Europe v Commission*). The essence of these arrangements is reducing uncertainty over the future conduct of competitors. Competition law prohibits such coordination as it impairs the very independence of market behaviour: each economic operator must determine by itself the policy he intends to adopt on the common market (*Joined cases 40 to 48, 50, 54 to 56, 111, 113 and 114-73, para 173*). Conceptually, such coordination is a form of information exchange that can occur directly between competitors or indirectly through a third party intermediary, including platforms, online tools, and algorithms. The reason for information exchange may be attributable to a regulatory policy of market transparency. The case concerning information exchange among Portuguese banks offers a fitting illustration, where some of the information exchanged was subject to disclosure under national consumer law obligations (*Case C-298/22 Banco BPN/BIC Português SA and Others v Autoridade da Concorrência, para 82*). As the Court pointed out, however, such mandated information exchange cannot infringe Article 101 TFEU in so far as it has no influence on the market beyond that already caused by compliance with regulatory obligations (paras 83-84). The national court upheld the infringement, rejecting the

proposition that information at issue concerning prices, quantities, costs, and demands merely replicated the data required to be disclosed under national law. The distinction between information exchange required by regulation and information exchange that goes beyond what is necessary is not an easy one to draw. The difficulty becomes particularly visible when and if compliance itself is expected to be a collective exercise.

Recent EU digital and information law initiatives such as the GDPR, but even more so the DSA and the EU AI Act, rely heavily on industry participation and knowledge to translate legal obligations into feasible and meaningful compliance frameworks. The concern is that this encouraged cooperation has a serious potential to reduce precisely the uncertainty between undertakings that competition law means to protect. The EU increasingly makes compliance a collective exercise and, in some fields, a preferred regulatory technique, while leaving Article 101 to operate largely as an external constraint on cooperation rather than as a key principle of its institutional design. This post develops the argument in three steps. It first outlines a regulatory background featuring intentional reliance on collective compliance as a regulatory approach (section A). It then examines how information exchange under consideration engages Article 101 and relevant case law (section B) and offers concluding remarks (section C).

A. Collective compliance

Collective compliance is not new. EU law has long relied on codes, voluntary agreements, and various forms of self-regulation to turn regulatory provisions into operational practices. The institutional formats and actual success of such compliance initiatives have, however, varied. The Audiovisual Media Services Directive 2010/13, for example, gave rise to a range of national self- and co-regulatory schemes, particularly in the field of advertising. The Platform-to-Business Regulation 2019/1150 envisaged the development of industry codes of conduct, although that ambition remained largely unrealised. Regulation 2018/1807 on the free flow of non-personal data instructed the Commission to encourage and facilitate Union-level self-regulatory codes on cloud-provider switching and data portability. The resulting SWIPO codes were produced but saw limited uptake and focused primarily on pre-contractual transparency rather than on the economic and technical dimensions that made switching difficult in practice. Against this background, more recent information law initiatives appear more successful in institutionalising collective compliance through attracting significant market participation and

producing codes and structures for their implementation and reporting. Codes of conduct (e.g. Articles 45-47 DSA) and codes of practice (Article 56 AI Act) are a case in point.

One of the key reasons behind a regulatory appeal of collective compliance is that it constitutes an information-producing institution on its own. The works on economics of regulation have long treated information asymmetry between regulators and regulated firms as one of the central challenges of regulatory design. Firms typically have more accurate and privileged information about the regulated industry, including, for example, market conditions, technological developments, and anticipated costs of compliance. As regulators are challenged with setting an appropriate level of care and compliance expectations, collective forums may provide a means through which at least some of this information could be learnt and rendered into actual practices. From the perspective of firms, participation in collective compliance may, among other things, provide access to knowledge that reduces duplication efforts of finding working compliance solutions. At the same time, however, the very information-producing function of collective compliance that makes it an attractive regulatory technique may turn it into a stable institutional process for producing and circulating regulatory knowledge among competitors at the expense of strategic uncertainty about competitors' conduct.

B. Assessment standard

As elucidated above, information exchange among competitors is not inherently unlawful: it may produce significant economic benefits (Revised Horizontal Guidelines, 2023, para 373). Reliable market information can be helpful in planning production, investment, and innovation decisions. It can also be critical for increasing customers' awareness and reducing consumer search costs. A certain level of transparency is therefore not only compatible with competition. It may very well be a condition of effective competition. The difficulty lies elsewhere. In a data-driven and AI-enabled and benefiting economy, digital markets are fast-moving and greatly unpredictable, with substantial investment commitments often made before technological paths, consumer preferences, and regulatory expectations become clear. Compliance choices may then become notable non-price parameters of competition. As was already recognised by the EU Commission, compliance with privacy as a regulatory objective can be simultaneously an important parameter of competition and driver of consumer choice (e.g. Case M.8124 –

Microsoft / LinkedIn, para 350). A similar line of argument could be extended to the very technical dimensions captured by compliance vocabulary.

Items such as companies' internal risk assessments, model documentation, safety protocols and considerations, and implementation strategies may, in the context of tech regulation, be more commercially significant and revealing than their seemingly technical nomenclature suggests. A risk assessment (e.g. under Article 9 EU AI Act, Articles 34-35 DSA), for example, may refer to firms' perceived vulnerabilities and potential investment and resource allocation priorities. Model documentation concerns technical capabilities and limitations, the level of product maturity, as well as certain design choices (e.g. under Article 53 EU Act and Annex XI). Safety protocols and testing can be used as proxies for estimating companies' anticipated compliance costs (e.g. human reviews, mitigation and escalation algorithms), and performance thresholds (e.g. Article 11 and Annex IV of the EU AI Act). Implementation strategies, on the other hand, can provide intelligence about timing of the model release, anticipated product changes or external evaluations. Some of this information may qualify for trade secret protection under the EU Trade Secrets Directive, but not all of it will. The risk of losing such protection should thus not be assumed to eliminate the competition concern altogether. While confidentiality of information may be relevant for assessing the competitive significance of an exchange, particularly where competitors obtain information that is not publicly available (see, e.g. *Case C-298/22 Banco, para 84*, Revised Horizontal Guidelines, 2023, para 388*),* it is not, however, the status of this information per se that triggers Article 101 application. For Article 101 purposes, as discussed, the key consideration is whether the exchange of such information reduces the strategic uncertainty about competitors' conduct and reduces parties' independent decision-making.

The assessment is contextual and is carried out on a case-by-case basis. Some types of data has more readily reflected Article 101 concerns (Revised Horizontal Guidelines, 2023, para 385), especially as illustrated by cases involving regular meetings in regularly booked hotel rooms and handwritten notes recording prices, production costs, and turnovers. In digital markets, however, information disclosed in discussions about compliance choices may provide indicators of a firm's market position and strategy that are comparable in commercial significance to expected output and production costs in traditional industries. From the case

law, this information might, in principle, fall under the "restriction-by-object" category (Revised Horizontal Guidelines, 2023, para 414). The Commission's *Car Emission case* (AT.40178), for example, concerned companies' cooperation on technical aspects of cars' emission technology, in particular a diesel exhaust-cleaning system (SCR) that used a special liquid (AdBlue) to reduce nitrogen oxide pollution. Specifically, there were DAIMLER, VW, and BMW that met in technical groups and coordinated car tank sizes and distances between refills, as well as exchanged information about anticipated average AdBlue consumption. As the Commission pointed out, such cooperation created "a high degree of transparency" regarding companies' current and future conduct on the market (recital 107), including their plans concerning AdBlue technology and the possible early fulfillment of upcoming emissions requirements (recital 84). By its very nature, the companies' conduct was liable to restrict competition on product characteristics and to limit choice for consumers (recital 124). The Commission specifically emphasised that the coordination at hand concerned not only compliance with regulatory requirements but also the competitive potential of exceeding them (recital 128). In other words, the cooperation sought to reduce the potential of one or several manufacturers gaining a competitive advantage by offering a more convenient or environmentally better solution. A related concern emerged in the *Trucks case* (AT.39824) where European truck manufacturers were found to have coordinated not only on price-related information but also on the timing of the introduction of emission technologies under EURO 3 to 6 standards and on the passing the associated costs to consumers. Applied to information law codes, relevant discussions, by analogy, could be around disclosure on how the AI ACT compliance costs will be reflected in API or enterprise pricing or how DSA ad-repository costs will be recovered.

Overall, as applying these cases to the DSA and AI compliance discussions in particular, the challenge is that the respective work does not merely define a minimum standard of safety, transparency or privacy, but has the potential to create an industry understanding of what is enough. Thus, the respective discussions that converge on the acceptable level of watermarking, copyright diligence, or risk mitigation may suppress competition on better offerings regarding safety, accountability, and overall compliance approaches. Even when and if no common understanding is formed, repeated exchanges may still pose a "restriction-by-effect" risk as they, by their function, seek to increase transparency and thus remove the competitive uncertainty. The assessment is, again, contextual, but is also counterfactual (

Revised Horizontal Guidelines, 2023, paras 421-424). In the context of compliance collaboration, the relevant enquiry should then ask what rivals would have known absent the collective compliance discussion in a particular case. Depending on attributes such as market concentration, the share of the market represented, frequency and granularity of interactions, a process that reveals, for example, AI model readiness, technical design choices and constraints, may provide competitors with substantially greater intelligence over one another's capabilities and likely conduct. Even incremental transparency in these settings may have an effect of reducing uncertainty over market participants' responses and may also weaken incentives to compete through, for instance, superior technical performance or more advanced or ambitious compliance solutions.

That is not to say that the information exchange would be necessarily unlawful in this case: the application of the exception under 101(3) rests on proving that the cooperation in question is likely to give rise to pro-competitive effects (Revised Horizontal Guidelines, 2023, paras 35-36). The regulatory push for codes of conduct and collective compliance exercises may provide a stronger conceptual basis for some of the conditions under Article 101(3), as the underlying purpose of these undertakings is to decrease uncertainty over compliance expectations and, as discussed, reduce duplication of efforts in finding industry-wide solutions. These gains could reasonably be expected to be translated into safer, perhaps cheaper or environmentally friendlier goods and services for consumers. The more difficult questions under 101(3), however, concern indispensability and preservation of competition. The respective enquiries demand attention to issues like, for example, the nature, frequency, and degree of information sharing actually necessary to achieve claimed efficiencies, and, second, to whether cooperation does not preclude meaningful competition on important parameters. Arguably, these attributes are particularly challenging to supervise as recent EU information law initiatives are not merely forums for coordinating legal interpretation. They are designed to systematically generate shared compliance knowledge, and where this compliance intelligence comes to shape what counts in practice as sufficient compliance, the respective cooperation begins to resemble a standard-setting process rather than just an ancillary information exchange. For standardisation, Article 101 already offers a principle of institutional thinking: the acceptability of the output is greatly conditioned on the design of the process through which it is produced. This insight matters especially here. Article 101 safeguards on

participation, information flows, and decision-making should be detailed *ex ante* in each compliance forum's governance structure, not merely as a "without prejudice to competition law" clause.

C. Concluding remarks

Existing DSA practice provides a useful but relatively limited starting point: the Disinformation Code and the Illegal Hate Speech Online+ Code have been incorporated into the DSA framework and accompanied by certain forms of reporting and auditing, where applicable (e.g. Article 17 of the EU Commission Delegated Regulation 2024/436). The subject matter of those codes does not necessarily raise the issue of collective compliance reaching into companies' prospective future technological and commercial choices as of yet. However, Article 45(2) anticipates precisely that possibility. In formulating governance rules for those cases of systemic risk compliance, particular attention should then be paid to (i) explicitly and clearly defining the regulatory question and equally what falls outside it; (ii) identifying the exact information needed and how that information should be obtained; (iii) recording what dimensions remain for individual decision-making of companies involved. Thus, while a common methodology for measuring exposure of a particular content or minimum risk-mitigation scenarios may be discussed collectively, more competition-sensitive information such as, for example, internal exposure rates and effectiveness of testing protocols should be submitted to an independent intermediary, and where appropriate, distributed only in aggregated form (e.g. data on the prevalence of the risk across platforms). At the same time, choices concerning the technical means of mitigation or timelines and resource allocations should remain individual.

The need for this kind of analytical proactive differentiation becomes even more acute under the AI Act. The GPAI Code of Practice is not just about administrative reporting: its implementation created a stand-alone Signatory Taskforce, chaired by the AI Office, which may facilitate discussions not only on the Code per se, but also on technological trends and future risk developments, including, for example, algorithmic efficiency, compute and energy use. Publicly available information on the Taskforce functioning suggests, first, that discussions have already moved to issues of data curation, post-market model-use information and

“marginal risk” clauses, matters closely related to technological trajectories, risk tolerance, and prospective deployment measures. At the same time, even though the meetings’ records demonstrate a principled awareness of the need to separate collective regulatory information from the data at an individual level, it is unclear whether and how exactly this distinction would be rendered into a systematic ex ante framework governing the direction and granularity of information flows, as well as the scope of individual decision-making capacity left. This uncertainty matters. As these forums are themselves institutionally endorsed to advance the effectiveness of compliance, the effectiveness of compliance with competition law should not be treated as an afterthought.

AVAILABLE AT

https://europeanlawblog.eu/collective-compliance-at-the-expense-of-competitive/

CC BY-SA 4.0