POLICY BRIEF

Soft Law, Hard Risks?

Co-Regulation and Risk Mitigation Under the Digital Services Act

Lena-Maria Böswald

November 19, 2025

Tech analysis and policy ideas for Europe

interface

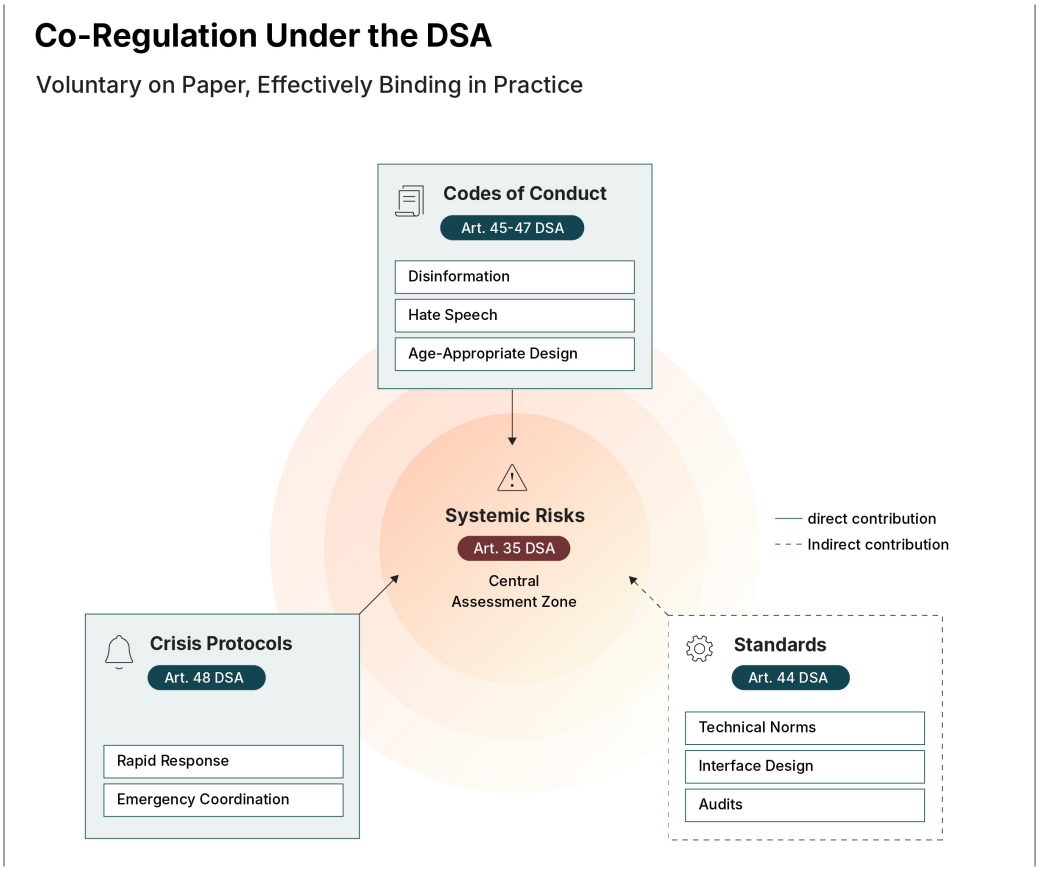
Table of Contents

Executive Summary

The EU's Digital Services Act (DSA) introduces a mix of **binding obligations and soft-law co-regulatory mechanisms** – notably *codes of conduct* (Art. 45–47), *crisis protocols* (Art. 48), and *industry standards* (Art. 44). These instruments are formally voluntary but operate within a hard-law due diligence framework that can have de facto legal consequences. Yet, questions remain about where exactly the boundary between voluntary cooperation and enforceable obligation lies, and how the DSA's regulatory grey zones can be approached in practice. The key challenge lies in determining how co-regulatory instruments can contribute to making the DSA function effectively as a risk-minimising regulatory framework, and what principles or measures are needed to ensure that they do so.

- ***Codes of conduct*** serve as a bridge between self-regulation and binding law, which can address underrepresented areas of the DSA and enable flexible responses to emerging harms. Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) that sign up and follow these codes are subject to independent audits. These audits make sure that platforms follow through on their commitments. Participation in codes is not mandatory, yet it demonstrates good-faith compliance, while non-signatories must prove they meet equivalent standards.
- ***Crisis protocols*** are voluntary mechanisms that the European Commission (EC) can develop, based on recommendations from the European Board for Digital Services, to respond to extraordinary crises in the online environment. The aim is to form a mechanism for rapid response during extraordinary circumstances (e.g., wars, pandemics). Platforms co-develop protocols with the EC and regulators to reduce systemic risks quickly; however, it is up to providers to participate voluntarily.
- Art. 44 encourages the EC and the Board of DSCs to support development of ***technical standards*** by organisations for standardisation, particularly regarding compliance with DSA provisions that involve the design of online interfaces and databases, as well as notice and action mechanisms, auditing methods and child protection. Providers of intermediary services can choose to adopt these standards, but their adoption does not presume compliance with the DSA.

Although co-regulatory mechanisms are presented as flexible and nonbinding, they can carry **de facto legal consequences** for VLOPs and VLOSEs. Signing up for co-regulatory mechanisms may be an incentive for industry players to mitigate risks under the DSA's systemic risk framework. Refusing to participate does not necessarily imply noncompliance, but VLOPs and VLOSEs that do not commit must explain clearly how they will meet their DSA obligations otherwise – and could risk infringement proceedings and fines. The possibility of fines further incentivises genuine participation.



This raises serious questions about whether co-regulatory mechanisms truly can be called voluntary instruments. However, without stronger monitoring, the implementation of co-regulatory mechanisms risks remaining performative rather than impactful; **they need proper monitoring and compliance assessment**.

A core concept of the DSA is **systemic risks**, which require VLOPs and VLOSEs to identify, assess, and mitigate risks arising from how their services are designed and operated. VLOPs and VLOSEs' compliance with codes of conduct and crisis protocols may be regarded as an appropriate risk mitigation measure under Art. 35, but participation in and implementation of such instruments does not in itself presume compliance with the DSA. This is an important distinction, as it allows the EC some leeway in deciding whether the level of commitment to the respective mechanism is compliant with the DSA's risk mitigation framework. In contrast, technical standards play only an indirect, supportive role in risk reduction. Ultimately, while co-regulation offers a promising framework for addressing systemic risks, its effectiveness depends on **measurable outcomes and consistent monitoring.**

Despite their potential to narrow down systemic risks (codes of conduct), enable faster, coordinated responses (crisis protocols) and promote comparability and

consistency across platforms (standards), the effectiveness of co-regulatory instruments remains limited by opaque drafting processes, platform withdrawals, inconsistent monitoring, incomplete reporting and uneven stakeholder participation. The EC's dual role as facilitator of co-regulatory mechanisms and enforcer further complicates matters. To ensure that co-regulation fulfils its intended purpose and strengthens the DSA's governance model, the following policy measures are recommended:

- **Soft law must complement, not replace binding regulation** — voluntary measures alone cannot change platform behaviour without clear assessment and enforcement mechanisms.
- **Independent monitoring with clear, measurable indicators** is needed to evaluate impact, not just procedural compliance.
- **Civil society participation** must be strengthened to guarantee inclusive and transparent multi-stakeholder engagement, beyond symbolic consultation.
- **Codes of conduct could serve as a best practice** for consistent risk mitigation for code-specific risks, guiding audits and helping align platforms' practices with DSA obligations.
- **Robust monitoring frameworks** are essential — a clear allocation of resources and impact assessment framework helps effective oversight.
- **Audits need to have a clear framework,** as no consistent way to evaluate the quality of audits exists currently.
- **Crisis preparedness and rapid-response protocols** should be integrated into risk governance to ensure platforms can act swiftly and consistently in emergencies.

Introduction

With the Digital Services Act (DSA), the European Union (EU) is experimenting with a mix of hard and soft regulations.[1] This rulebook for online platforms, search engines and marketplaces is a binding EU law, while several voluntary instruments that still can pose legal consequences are introduced simultaneously. These mechanisms include 'codes of conduct' (Article 45), 'crisis protocols' (Article 48), and 'standards' (Article 44). Together, they contribute to a long list of so-called co-regulatory schemes that already exist in the tech sector. The DSA's co-regulatory model marks a broader shift in the EU's digital policy towards combining binding rules with collaborative and flexible governance. This approach recognises that in fast-changing technological environments, traditional regulation alone is often too static for the cat-and-mouse game of regulation, technological development and effective oversight.

1 Carl Vander Maelen, "Hardly Law or Hard Law? Investigating the Dimensions of Functionality and Legalisation of Codes of Conduct in Recent EU Legislation and the Normative Repercussions Thereof", *European Law Review 47* (6) (January 2022), pp. 752–72.

Co-regulation is a governmental strategy that establishes a non-state regulatory regime engaging multiple stakeholders in which rules are negotiated by the regulator and those subject to them. With tech regulation, this often includes industry representatives, consumer organisations, civil society, public interest groups, and – depending on the subject – advertisers. The idea of co-regulatory instruments under the DSA is that they will serve due diligence obligations and provide more detail on some of the DSA's transparency requirements. Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) can choose to commit to such mechanisms. It will become clear below that signing up for co-regulatory mechanisms may be an incentive for industry players to mitigate risks under the DSA's systemic risk framework. If they do sign up, their compliance with the DSA will be monitored by independent auditors under Art. 37 — just as if they were following binding DSA rules. Refusing to do so does not necessarily imply noncompliance, but VLOPs and VLOSEs who do not commit must explain clearly how they will meet their DSA obligations otherwise – and could risk infringement proceedings and fines.

Therefore, the DSA's balance lies in a binding regulation that delegates parts of its implementation to nonbinding, co-regulatory instruments.[2] What remains uncertain is how this 'voluntary' and 'mandatory' combination works in practice. It is also unclear how codes of conduct, the most prominent co-regulatory mechanism defined in the DSA, will relate to the other instruments that the regulation calls for, such as industry standards and crisis protocols.

This policy brief aims to shed light on how effective co-regulatory mechanisms are under the DSA in ensuring accountability and risk mitigation. First, it maps co-regulation's role under the DSA and how mechanisms may be de facto binding, demonstrating that the regulation contains provisions for their legal enforcement. Second, this paper outlines how co-regulatory frameworks can be used to mitigate risks under Art. 35, and identify where their potentials and limitations lie. Third, it compares co-regulation under the DSA with similar mechanisms in the General Data Protection Regulation (GDPR) and Artificial Intelligence (AI) Act to outline development of co-regulatory instruments in recent years. Fourth, it aims to list concrete measures for regulators and platforms on what needs to be done for co-regulation to work effectively in practice.

2 Rachel Griffin, "Codes of Conduct in the Digital Services Act: Functions, Benefits & Concerns", *Technology and Regulation* (September 2, 2024), pp. 175-177.

Why Co-Regulation at All? Soft Law Paths to DSA Compliance

Under the DSA, co-regulatory mechanisms are embedded explicitly in Articles 44-48, encompassing industry standards, codes of conduct, and crisis protocols. These mechanisms are voluntary in form but operate within a legally binding due diligence architecture, in which compliance may influence regulatory intervention further. The European Commission (EC) plays a coordinating and endorsing role while Member States' authorities, such as Digital Services Coordinators (DSCs) and the European Board for Digital Services, at least for crisis protocols, ensure national implementation and cross-border coherence. In practice, this design situates co-regulation at the intersection of soft and hard law: Private actors retain flexibility to shape co-regulatory mechanisms, but under a regime of structured oversight by both the regulator and civil society stakeholders aimed at ensuring transparency, accountability and fundamental rights protection. Now that we have gained an overview of co-regulation mechanisms in general, we will examine three different instruments in detail: codes of conduct, crisis protocols, and standards.

Codes of Conduct

Codes of conduct under the DSA are voluntary but closely linked to platforms' broader compliance duties. They are designed to bring more attention to topics that the DSA does not fully address and translate abstract legal requirements into concrete, actionable measures. Given their 'soft law' character, codes can address content that is technically legal but harmful (e.g., disinformation), including content that lacks a clear legal definition, and respond quickly to new risks as they arise. In this way, codes occupy a middle ground between voluntary self-regulation and mandatory rules, helping implement legal objectives through industry-specific measures.

Platforms are **not obligated** to join, but participation can demonstrate good faith and compliance efforts, as platforms that do not sign the code still are required to demonstrate that they are taking equivalent measures against systemic risks, such as disinformation or illegal hate speech, to demonstrate DSA compliance. Platforms or search engines that sign up and follow these codes — particularly VLOPs and VLOSEs — are subject to independent audits under Art. 37(1,b). These audits, similar to those for risk assessments and mitigation measures, verify that platforms follow through on their commitments. If problems are flagged, platforms have one month to act on the auditor's recommendations and report back to the EC.

Currently, no standardised method for auditing compliance exists, as previous codes of conduct have not been subject to independent audits before and have used different methods to measure efficiency in the past, depending on the code topic. It remains unclear how voluntary commitments interact with mandatory legal obligations under the DSA.

The DSA highlights specific areas in which codes of conduct are expected (Recital[3] 104), including disinformation, manipulative or abusive activities, any adverse effects on minors, and specific types of illegal content. While codes on disinformation and age-appropriate design are relatively straightforward because both are viewed as key policy priorities by the EC, defining 'manipulative or abusive activities' is more complex and open to interpretation.

Codes of conduct must be developed through multi-stakeholder processes involving platforms, industry actors and potentially civil society as outlined in Art. 45(2). They are not limited to VLOPs and VLOSEs but also can apply to other online platform providers and intermediary services. The EC and Board do not draft these codes; their role is to encourage and facilitate the process and ensure the codes align with EU citizens' needs and interests.

Overview of Already Existing Codes of Conduct

Some codes addressing platform regulation already had been developed before the DSA fully came into force – on a voluntary basis by the industry, though with EC encouragement and involvement.[4] This is important, as already existing codes – the Code of Conduct on Combatting Illegal Hate Speech and the former Code of Practice on Disinformation – have been 'squeezed' into the DSA's framework instead of new codes emerging from the regulation itself. The conversion to a code of conduct under the DSA means the codes are more authoritative. As a consequence, establishment of new codes that are fully developed under Art. 45 DSA will become an interesting case study for assessing how closely tied they are to legal enforcement of the DSA.

Code of Conduct on Disinformation

First signed in 2018, the Code of Practice on Disinformation (CoP) – based on an EU Action Plan and strengthened in 2022 – was 'the first time worldwide that industry

3 Recitals, often known as preambles, are found at the beginning of the DSA and offer the possibility to provide context and background information to the regulation.

4 Teresa Quintel and Carsten Ullrich, "Self-Regulation of Fundamental Rights? The EU Code of Conduct on Hate Speech, Related Initiatives and Beyond," in *Fundamental Rights Protection Online*, ed. Bilyana Petkova and Tuomas Ojanen (Cheltenham: Edward Elgar Publishing, 2020).

agrees, on a voluntary basis, to self-regulatory standards to fight disinformation'.[5] It is a voluntary commitment initiated by the EC and signed by major tech companies, setting out rules on how platforms should combat dis- and misinformation. For example, these standards include transparency requirements, enforcement of community guidelines and the obligation to cooperate with fact-checkers and researchers. This translates into the EC pushing platforms to combat disinformation, but as main drafters, they predominantly set their own self-regulatory obligations.

Disinformation has been a political priority since the Cambridge Analytica scandal in 2018, but expanding formal legal regulation is viewed widely as problematic due to freedom-of-expression concerns. Thus, importance is attached to soft law measures such as self-regulatory codes of conduct. The DSA does not explicitly define systemic risks related to disinformation or how to measure them, so the Code outlines concrete measures that signatories should apply to combat these risks.

On 13 February 2025, the EC and European Board for Digital Services formally endorsed integration of the CoP into the DSA framework, thereby converting it into a Code of Conduct (CoC) under the DSA. Effective 1 July 2025, the EC integrated the Strengthened CoP into the DSA and transformed the code from a voluntary agreement into a cornerstone of the regulation – 'a shift from the current flexible self-regulatory approach to a more co-regulatory one'[6]. In doing so, the Code can become a relevant benchmark for determining DSA compliance under Art. 35 of the DSA. Although the Preamble to the 2022 Strengthened Code of Practice on Disinformation emphasises the code's voluntary nature, its appointment as a CoC bears potential implications for enforcement actions against online platforms that fail to adhere to its provisions.

Structure and Oversight

The former CoP set up an additional oversight mechanism in the form of a permanent task force chaired by the EC. Code compliance currently is evaluated via self-declaration, encompassing 44 commitments implemented through 128 specific measures. Compliance with these voluntary commitments is monitored by digital media observatory hubs in 15 member states.

Code of Conduct + on Combatting Illegal Hate Speech

To respond to the proliferation of racist and xenophobic hate speech online, the EC and four major IT companies (Facebook, Microsoft, Twitter and YouTube) unveiled a

---

5 European Commission, "Code of Practice on Disinformation", European Commission, September 26, 2018, accessed October 17, 2025, https://digital-strategy.ec.europa.eu/en/news/code-practice-disinformation

6 European Regulators Group for Audiovisual Media Services (ERGA), *ERGA Report on Disinformation: Assessment of the Implementation of the Code of Practice* (May 2020), p. 52.

Code of Conduct on countering illegal hate speech online in May 2016. The original Code of Conduct was designed to combat the spread of illegal hate speech online through voluntary measures. Since then, Instagram, Snapchat, Dailymotion, Jeuxvideo.com, TikTok, LinkedIn and, in spring 2022, Rakuten Viber and Twitch joined the Code. The Code of Conduct+ (CoC+), now embedded in the DSA, strengthens enforcement mechanisms and increases platform accountability in identifying, moderating, and removing illegal hate speech in compliance with EU and national legal frameworks. The updated version imposes stricter obligations on online platforms regarding detection and removal of illegal hate speech. It also ensures that content moderation processes are timely and effective, preventing proliferation of hate speech before it causes harm.

The CoC+ is based on close cooperation between the EC, platforms, CSOs and national authorities. All stakeholders meet regularly under the umbrella of the High-Level Group on combating hate speech and hate crime to discuss challenges and progress.

Structure and Oversight

The EC continues monitoring the implementation of the CoC+. The Code takes the form of five commitments and two annexes. The signatories are assessed annually, with seven rounds of compliance monitoring completed thus far. The Code's annexes outline the annual monitoring exercise's methodology, whereby monitoring reporters report alleged illegal hate speech in online content through designated reporting processes for a period of a maximum of six weeks, with key performance indicators (KPIs) listed. Civil society was reported not to be involved in the 2016 Code of Conduct on Countering Illegal Hate Speech Online; therefore, its involvement was strengthened with the introduction of an expert exchange forum that provides feedback on the updated CoC+.

Other Codes of Conduct

Within the framework of the Digital Services Act's provisions on Codes of Conduct, the EC was expected to encourage development of two additional voluntary codes by 18 February 2025. However, this did not occur.

Codes of Conduct on Online Advertising

The first code, mentioned under Art. 46, is the Code of Conduct for Online Advertising, which aims to enhance transparency and fairness throughout the online advertising value chain. Ad industry representatives, encouraged by the EC and supported by CSOs, are supposed to develop these codes, with an emphasis on transparency regarding ad labels, ad repositories and how data are monetised in online ad markets. Particularly for ad tech companies that sign on to the codes but are otherwise not covered by the DSA, as they do not fall under the regulatory regime, no sanctions are envisioned. Thus, few incentives for compliance exist.

Codes of Conduct for Accessibility

The second code, as provided for in Art. 47, is the Code of Conduct for Accessibility, designed to improve access to online services for people with disabilities. Such a code should promote full, effective, and equal participation in online services for everyone. Surprisingly enough and without any explanation or substantiation in the text, the EC has requested KPIs and reporting commitments for codes of conduct under Art. 45, but not under Art. 46 and Art. 47.

Code of Conduct on Age-Appropriate Design

The Code of Conduct for Age-Appropriate Design has been in the drafting stage since 2023, with a dedicated expert group working on a draft.[7] Although its drafting and monitoring process seems to follow a slightly different approach than other codes, with the establishment of an expert group from the very beginning, the EC similarly mentions that the code will build on the regulatory framework provided in the DSA and assist with its implementation.

Crisis Protocols

The DSA has introduced significant rules on measures that platforms must adopt in times of crisis, as set out under provisions on the crisis response mechanism (Art. 36) and voluntary crisis protocols. In addition to codes of conduct, crisis protocols (Art. 48) are another instrument of co-regulation within the DSA framework. These are voluntary mechanisms that the EC can develop, based on recommendations from the European Board for Digital Services, to respond to extraordinary crises in the online environment.

However, no examples of fully activated crisis protocols exist so far. They are intertwined with the swiftly added and heavily criticised crisis response mechanisms that have not been enforced to this date.[8] Both the crisis response mechanism and voluntary crisis protocol in the DSA have sparked significant debate among civil society.[9] Introduced amid Russia's invasion of Ukraine, these provisions aim to address platforms' roles in spreading information during crises – both reliable information and mis- and disinformation. However, civil society groups

7 European Commission, "Crafting of the Code of Conduct on age-appropriate design kicks off today", European Commission, July 12, 2023, accessed 17 October 2025, https://digital-strategy.ec.europa.eu/en/news/crafting-code-conduct-age-appropriate-design-kicks-today

8 European Parliament, "Answers given by Executive Vice-President Virkkunen on behalf of the European Commission", European Parliament, April 24, 2025, accessed 20 October 2025, https://www.europarl.europa.eu/doceo/document/E-10-2025-000852-ASW_EN.html

9 EDRi, "Public Statement: On new crisis response mechanism and other last minute additions to the DSA, EDRi, April 12, 2022, accessed October 20, 2025, https://edri.org/wp-content/uploads/2022/04/EDRi-statement-on-CRM.pdf

raised concerns in April 2022 that the EC's broad and unilateral power to declare a state of crisis, coupled with vague definitions and no time limits, could undermine the rule of law, legal certainty, and freedom of expression by enabling extended or excessive restrictions on information. As this paper focuses on co-regulatory instruments, we will dive a little deeper into the concept of voluntary crisis protocols.

The initiative for the protocols comes from the EC, which – based on the European Board for Digital Services' recommendation – may initiate development of voluntary crisis protocols to address crises in the online environment (Art. 48). As a consequence, the EC must determine what constitutes a crisis based on feedback from national regulators. The DSA keeps the definition vague, with an emphasis on the threat of a crisis, as Art. 48 refers to 'situations [...] strictly limited to extraordinary circumstances affecting public security or public health'. The aim of crisis protocols, as outlined in Art. 48, is to form a mechanism for rapid response during extraordinary circumstances (e.g., wars, pandemics), similar to the rapid response mechanism under the Code of Conduct on Disinformation that focusses on threats during election cycles. The EU Commission shall encourage VLOPs, VLOSEs and other platforms to participate in the drawing up, testing, and application of these crisis protocols. Thus, platforms co-develop protocols with the EC and regulators to reduce systemic risks quickly; however, it is up to providers to participate voluntarily.

Recital 108 of the DSA emphasises that the EC specifically envisions activation of and may initiate the crisis protocol in scenarios requiring a rapid, collective and cross-border response, such as when 'online platforms are misused for the rapid spread of illegal content or disinformation or where the need arises for rapid dissemination of reliable information.' The measures to be taken once the crisis protocol has been activated are strictly limited to what is 'necessary' under Art. 48(4,d). Under Art. 48(4,e), the EC 'shall aim to ensure' that crisis protocols 'set out clearly' safeguards to address any 'negative effects on the exercise of the fundamental rights enshrined in the Charter, in particular the freedom of expression and information'.

The extent to which the EC's role is actually defined is up for interpretation by the legislator, as the wording suggests that the Commission should at least *encourage* and *facilitate* the drafting of crisis protocols. However, it also could be the driving force in determining the protocol. Of course, given the explicitly voluntary nature of the provider's participation, the provider is, in theory, free not to accept such a strong role for the EC or to disagree with the protocol, as the provider can withdraw at any stage of the process. Whether this will take place in practice, once the crisis protocol is up for discussion, has yet to be seen, given the increasing public pressure on providers and the voluntary but binding nature of crisis protocols, which will be

discussed in the following section.

Measures that are to be undertaken when setting up crisis protocols[10] are, amongst others:

1. Displaying information on the crisis 'provided by Member States' authorities or at Union level' or 'other relevant reliable bodies'
2. Adapting resources to needs arising from the crisis

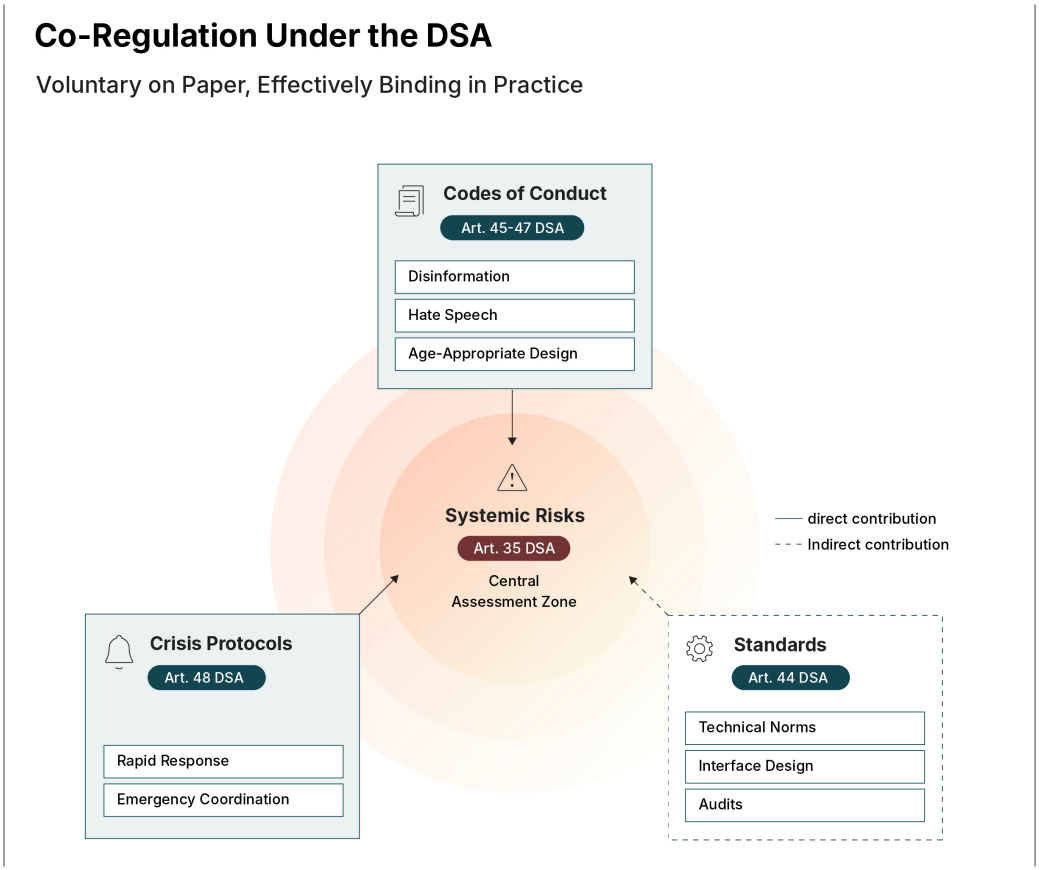
Here, according to the DSA Observatory, a question arises as to who defines what information will be displayed during a crisis. Art. 48 DSA does not clarify who decides on the actual policies, nor does it specify what content can be qualified as trustworthy. The last possible measure that Article 48(2,c) states – the adaptation of resources – leaves room for a lot of questions as well. As crisis protocols have not been used in practice yet, these questions remain unanswered so far, but will be important in case of activation.

Standards

Finally, technical standards also fall under the triad of co-regulatory instruments under the DSA. Art. 44 encourages the EC and the European Board for Digital Services to support development of technical standards by organisations for standardisation, particularly regarding compliance with DSA provisions, focussing on the design of online interfaces and databases, as well as notice and action mechanisms, auditing methodologies and child protection. Codes of conduct and crisis protocols' connection to any future voluntary industry standards, which the DSA also calls for, is unclear. The EC can support and promote only the development and implementation of standards. Recital 102 specifies that 'the industry can help develop standardised means to support providers of intermediary services in complying with this Regulation'. Providers of intermediary services can choose to adopt these standards, but their adoption does not presume compliance with the DSA.[11]

10 See Doris Buijs and Ilaria Buri, "The DSA's Crisis Approach: Crisis Response Mechanism and Crisis Protocols," *DSA Observatory*, February 21, 2023, accessed October 20, 2025, https://dsa-observatory.eu/2023/02/21/the-dsas-crisis-approach-crisis-response-mechanism-and-crisis-protocols/

11 see Recital 102 DSA



Voluntary, Until It Isn't: How Soft Law Supports the DSA's Implementation

The DSA and EC present co-regulatory tools as voluntary forms of self-regulation. In theory, this approach blends legal enforceability with flexibility. In reality, several mechanisms in the DSA make voluntary soft law *de facto* binding.

Codes of Conduct		
Codes of conduct	Art. 45(2) DSA	Where significant systemic risk within the meaning of Article 34(1) emerge and concern several very large online platforms or very large online search engines, the Commission may invite the providers of very large online platforms concerned or the providers of very large online search engines concerned, and other providers of very large online platforms, of very large online search engines, of online platforms and of other intermediary services, as appropriate, as well as relevant competent authorities, civil society organisations and other relevant stakeholders, to participate in the drawing up of codes of conduct, including by setting out commitments to take specific risk mitigation measures, as well as a regular reporting framework on any measures taken and their outcomes.

	Art. 45(4) DSA	In the case of systematic failure to comply with the codes of conduct, the Commission and the Board may invite the signatories to the codes of conduct to take the necessary action.
Mitigation of risks	Art. 35 (1), h DSA	Providers of very large online platforms and of very large online search engines shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 34, with particular consideration to the impacts of such measures on fundamental rights. Such measures may include, where applicable: (h) initiating or adjusting cooperation with other providers of online platforms or of online search engines through the codes of conduct and the crisis protocols referred to in Articles 45 and 48 respectively
Independent audit	Article 37(1) DSA	Providers of very large online platforms and of very large online search engines shall be subject, at their own expense and at least once a year, to independent audits to assess compliance with the following: (a) the obligations set out in Chapter III; (b) any commitments undertaken pursuant to the codes of conduct referred to in Articles 45 and 46 and the crisis protocols referred to in Article 48.
	Recital 103 DSA	The Commission and the Board should encourage the drawing-up of voluntary codes of conduct, as well as the implementation of the provisions of those codes in order to contribute to the application of this Regulation. The Commission and the Board should aim that the codes of conduct clearly define the nature of the public interest objectives being addressed, that they contain mechanisms for independent evaluation of the achievement of those objectives and that the role of relevant authorities is clearly defined. [...] While the implementation of codes of conduct should be measurable and subject to public oversight, this should not impair the voluntary nature of such codes and the freedom of interested parties to decide whether to participate. In certain circumstances, it is important that very large online platforms cooperate in the drawing-up and adhere to specific codes of conduct. Nothing in this Regulation prevents other service providers from adhering to the same standards of due diligence, adopting best practices and benefitting from the guidelines provided by the Commission and the Board, by participating in the same codes of conduct.
Self- and co-regulatory agreements and risk mitigation	Recital 104 DSA	In particular, risk mitigation measures concerning specific types of illegal content should be explored via self- and co-regulatory agreements. Another area for consideration is the possible negative impacts of systemic risks on society and democracy, such as disinformation or manipulative and abusive activities or any adverse effects on minors. In relation to such areas, adherence to and compliance with a given code of conduct by a very large online platform or a very large online search engine may be considered as an appropriate risk mitigating measure. The refusal without proper explanations by a provider of an online platform or of an online search engine of the Commission's invitation to

		participate in the application of such a code of conduct could be taken into account, where relevant, when determining whether the online platform or the online search engine has infringed the obligations laid down by this Regulation.
	Strengthened Code of Practice: Preamble (h)	Actions under the Code will complement and be aligned with regulatory requirements and overall objectives in the Digital Services Act (DSA) once it enters into force. The DSA will set out a coregulatory framework, including through voluntary Codes of Conduct or other co-regulatory measures, aimed at addressing systemic risks by the Very Large Online Platforms, including those linked to Disinformation.
	Code of Conduct +: Preamble (f)	This Code aims to become a voluntary code of conduct under Article 45 of the DSA. It is in this spirit that the Signatories have agreed on this Code of Conduct+ (hereafter referred to also as "the Code"), identifying voluntary commitments aimed at creating a framework that facilitates the compliance with and the effective enforcement of the DSA in the specific area of illegal hate speech content, including new measures to address the most recent challenges and threats.
Crisis protocols		
Crisis protocols	Art. 48 (5) DSA	If the Commission considers that a crisis protocol fails to effectively address the crisis situation, or to safeguard the exercise of fundamental rights as referred to in paragraph 4, point (e), it shall request the participants to revise the crisis protocol, including by taking additional measures.
	Recital 108 DSA	"[...] the Commission may initiate the drawing up of voluntary crisis protocols to coordinate a rapid, collective and cross-border response in the online environment. [...] In light of the important role of very large online platforms in disseminating information in our societies and across borders, providers of such platforms should be encouraged in drawing up and applying specific crisis protocols. Such crisis protocols should be activated only for a limited period of time and the measures adopted should also be limited to what is strictly necessary to address the extraordinary circumstance.
Mitigation of risks	Art. 35 (1), h DSA	Providers of very large online platforms and of very large online search engines shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 34, with particular consideration to the impacts of such measures on fundamental rights. Such measures may include, where applicable: (h) initiating or adjusting cooperation with other providers of online platforms or of online search engines through the codes of conduct and the crisis protocols referred to in Articles 45 and 48 respectively
Compliance function	Art. 41 DSA	Compliance officers shall have the following tasks: (f) where applicable, monitoring the compliance of the

		provider of the very large online platform or of the very large online search engine with commitments made under the codes of conduct pursuant to Articles 45 and 46 or the crisis protocols pursuant to Article 48.

According to Article 45 (1), Sentence 1, codes of conduct are described as 'voluntary'. Furthermore, such codes' 'voluntary nature' and the freedom of choice regarding participation are expressly emphasised in Recital 103, Sentence 4 DSA, while emphasising the importance of cooperating in developing and adhering to specific codes.[12]

For platforms, codes of conduct provide both legal certainty in covering unspecified areas of the regulation and offer a way to demonstrate commitment to the DSA, even if Recital 104 DSA states that 'the mere fact of participating in and implementing a given code of conduct should not in itself presume compliance'. As already mentioned before, VLOPs and VLOSEs face strong incentives to comply with codes to prove they made an effort to comply with the regulation's risk mitigation framework. Furthermore, if they refuse to participate in response to an *invitation* from the EC, platforms risk infringement proceedings and fines.

As a drawback, the 'voluntary nature' of codes of conduct also allows VLOPs and VLOSEs to opt out of clauses they disagree with or they find compromising. A prominent example was the retreat of VLOPs and VLOSEs – including YouTube, Google and Microsoft – from, amongst other aspects, their fact-checking commitments made in the Code of Practice on Disinformation before it was officially integrated into the DSA as a Code of Conduct on 1 July 2025.[13] The main argument: Converting the Code would entail legal risks related to audits pursuant to Art. 37(1,b). However, this is not substantiated per se, because instead of working with an already existing framework of measures that the platforms helped shape, they resort to new measures that they must prove first to be compliant with the DSA's obligations. So far, the only case in which a platform dropped out of the 2022 Code of Practice completely was in 2023, when tech billionaire Elon Musk took over Twitter (now X).[14] Commenting on the decision, Věra Jourová, former EC Vice President for Values and Transparency, stated, 'I know the code is voluntary, but make no mistake: By leaving the code, Twitter [X] has attracted a lot of attention, and its actions and compliance with EU law will be scrutinised vigorously and

12 See Recital 103 DSA

13 Daniela Alvarado Rincón and Michael Meyer-Resende, "Big Tech Is Backing out of Commitments Countering Disinformation: What's Next for the EU's Code of Practice?", Democracy Reporting International, February 7, 2025, accessed October 24, 2025, https://democracy-reporting.org/en/office/EU/publications/big-tech-is-backing-out-of-commitments-countering-disinformation-whats-next-for-the-eus-code-of-practice

14 Natasha Lomas, "Elon Musk Takes Twitter Out of the EU's Disinformation Code of Practice," *TechCrunch*, May 27, 2023, accessed October 24, 2025, https://techcrunch.com/2023/05/27/elon-musk-twitter-eu-disinformation-code/

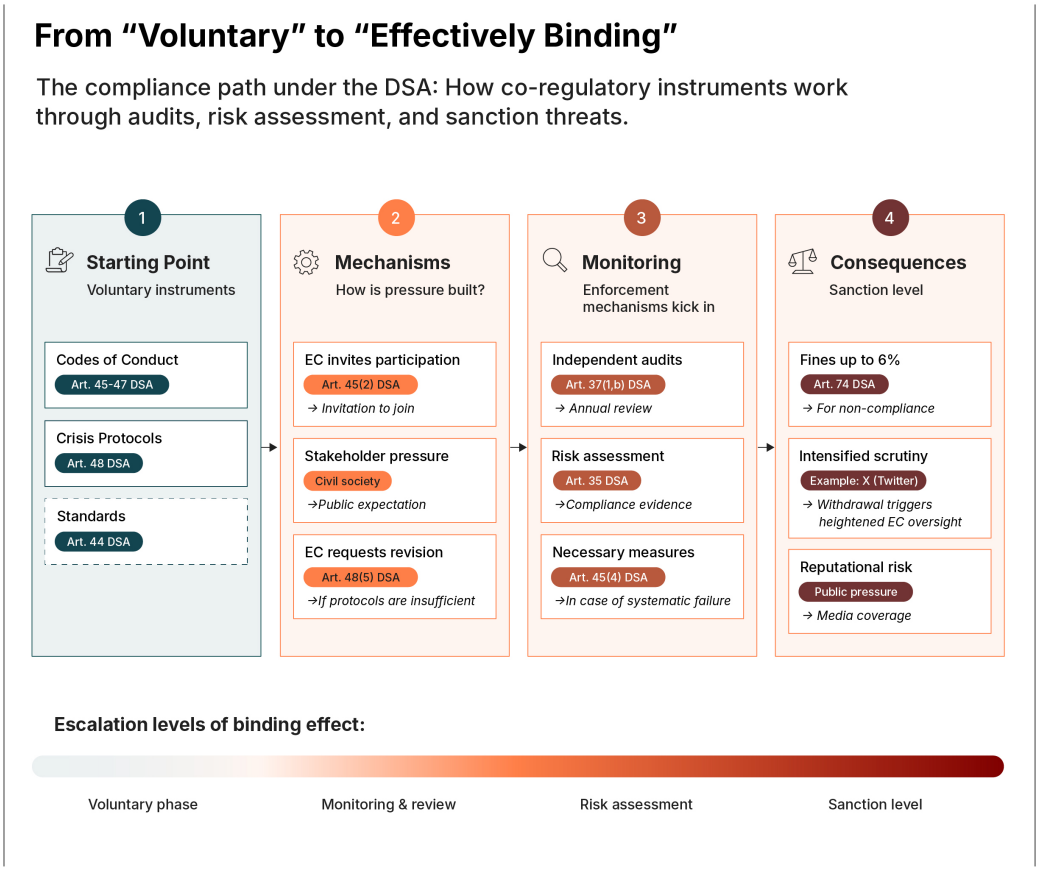
urgently'. Jourová's statement suggests that the EC will not shy away from treating noncompliance with 'voluntary' codes as a violation of Art. 35. So far, nothing has happened yet, as codes have not been audited yet and the data in transparency reporting have been lacking clarity. Once a platform chooses to adhere to codes of conduct under Art. 45-47 DSA, it is **expected** to respect the commitments outlined in the relevant code(s). While these commitments do not replace legally binding obligations under the DSA, they serve as a structured framework to help platforms align with regulatory expectations, particularly regarding risk mitigation.

As for crisis protocols, Art. 48(1) outlines their 'voluntary' nature. For VLOPs, VLOSEs and other platforms, the EC can only ask the platform to revise the protocol and/or ask for additional measures to be taken, but it cannot enforce any changes to the protocol or its measures according to Art. 48(5). Even though protocol participation will be overseen, its voluntary nature suggests that the drafting of and participation in crisis protocols cannot be forced.[15] For VLOPs and VLOSEs, however, noncompliance with the crisis protocols they have voluntarily adhered to can eventually lead to sanctions under the risk mitigation framework. Therefore, VLOPs and VLOSEs' adherence to a crisis protocol, similar to codes of conduct, may begin as voluntary, but noncompliance can pose detrimental consequences.

Standards are 'voluntary' according to Art. 44(1) and no further referral in the DSA renders standards binding.

Although the DSA's co-regulatory mechanisms are officially voluntary, except for technical standards, they operate within a hard-law due diligence framework that grants the EC leverage to translate noncompliance into legal consequences. Under Art. 45(2) and Art. 48(5), regulators can invite VLOPs and VLOSEs to participate in codes of conduct and crisis protocols, as well as ultimately determine whether platforms' efforts are sufficient to comply with Art. 35. Moreover, the DSA integrates reporting and auditing requirements (Art. 37-39) that reinforce indirect enforceability by exposing deficiencies in platforms' adherence to co-regulatory mechanisms. The possibility of fines under Art. 74 further incentivises genuine participation.

15 Marsch in Hofmann/Raue (Hrsg), *Digital Services Act: Gesetz über digitale Dienste* (2023).



This raises serious questions about whether co-regulatory mechanisms truly can be called voluntary instruments. In principle, co-regulatory mechanisms should lead only to a self-binding obligation. In the case of the DSA, the contradiction to the proclaimed 'voluntary nature' becomes even clearer in the provisions on systemic risk mitigation outlined in the following section. The factor that contributes most to a 'hardening of soft law'[16] is the possibility of sanctions, which can be imposed for noncompliance with the systemic risk framework. Creating de facto regulatory obligations on sensitive and politicised issues such as disinformation or systemic crises through informal industry negotiations, in which the EC exerts substantial influence, creates a certain potential for under-and over-removal of content, and we should be very mindful of what the effect could be if they are treated as de facto binding standards. However, co-regulatory mechanisms need proper monitoring and compliance assessment for signatories. **Without stronger monitoring, their implementation risks remaining performative rather than impactful.**

16 Tahireh Panahi and Andressa de Bittencourt Siqueira, "Soft Law, Hardcore? The Legal Enforcement of Codes of Conduct under the Digital Services Act," *Verfassungsblog*, June 3, 2024, accessed October 24, 2025, https://verfassungsblog.de/soft-law-dsa-co-regulation/

How Co-Regulation Contributes to Risk Mitigation Under Article 35 DSA

A core concept of the DSA, particularly for VLOPs and VLOSEs, is systemic risks: The regulatory framework revolves around identification, assessment and mitigation of risks arising from VLOPs and VLOSEs with over 45 million monthly EU users and linked to how their services are designed, operated, and used. The regime for VLOPs and VLOSEs goes beyond obligations related to individual content or users, imposing due diligence duties that require systemic changes. Central to this are Art. 34 ("Risk assessment") and Art. 35 ("Mitigation of risks"), which view VLOPs and VLOSEs as responsible for regularly assessing various systemic risks – albeit without clear definitions – and implementing mitigation measures. Co-regulatory mechanisms are key tools for VLOPs and VLOSEs in fulfilling these cornerstone obligations. Here is why:

The European Commission can, for instance, request a VLOP or VLOSE to participate in drafting a code of conduct under Art. 45(2) if significant systemic risks arise under Art. 34. However, the notion of risk remains vague. Terms like 'civic discourse,' 'electoral processes' and 'public security', as well as qualifiers such as 'foreseeable negative effect' are open to wide interpretation by regulators, companies, and the public. Even 'illegal content' is defined elsewhere, as what constitutes illegality is regulated in EU or national law. Consequently, companies must make best guesses about which risks are viewed as systemic and how to assess them, leading to inconsistent approaches across platforms. This uncertainty also may affect how the EC justifies VLOPs and VLOSEs' request for participation in codes of conduct that cover systemic risks, highlighting the need to monitor the EC's agenda-setting role in defining which systemic risks are to be addressed and ensure meaningful civil society involvement.

Co-regulatory instruments – codes of conduct and crisis protocols – can help platforms operationalise risk mitigation. While the EC has provided little clarity on the definition of 'systemic risk' in the DSA, co-regulatory instruments could fill this gap by setting out a structured, technical framework. For example, for codes of conduct, this includes specific performance indicators – both quantitative and qualitative – to help platforms mitigate disinformation risks and illegal hate speech more effectively. Platforms are expected to treat codes of conduct as industry best practice when selecting risk mitigation measures, report regularly on implementation, and measure progress against KPIs.

Although participation starts as voluntary according to Art. 45(1), systemic failure

to comply can trigger 'necessary measures' under Art. 45(4). The wording here remains rather vague, but it can be assumed from the context that the necessary measures imply compliance with the code of conduct, creating potential legal consequences under the DSA's risk mitigation framework in the event of noncompliance (Art. 74). In that sense, VLOPs and VLOSEs' adherence to codes of conduct may start as voluntary, but noncompliance can pose detrimental consequences. VLOPs and VLOSEs' compliance with codes of conduct may be regarded as an appropriate risk mitigation measure under Art. 35(1,h), but participation in and implementation of codes of conduct 'should not in itself presume compliance with [the DSA]' (Recital 104). This is an important distinction, as it allows the EC some leeway in deciding whether the level of commitment to the respective code of conduct is compliant with the DSA's risk mitigation framework. Interestingly, Art. 46 and 47, although codes of conduct, are not directly linked to the risk mitigation framework under Art. 35. Here, the question remains whether Recital 104 – in which codes of conduct are mentioned generally – outweighs a direct referral in Art. 35.

Similarly, crisis protocols require cooperation between platforms in response to risks, but ambiguity remains about what constitutes a 'systemic' crisis that is then effectively covered by the DSA's risk mitigation framework. Similar to codes of conduct, for VLOPs and VLOSEs, noncompliance with the crisis protocols they have voluntarily adhered to eventually can lead to sanctions under the risk mitigation framework.

In contrast, technical standards have no direct legal tie to risk mitigation, although they may reduce cross-platform risks indirectly (e.g., transparency in recommender systems or protection measures for minors.[17] Their potential contribution remains speculative until formal standards are established, yet one would assume that an industry-wide standard minimises the occurrence of cross-platform risks.

In summary, risk is the DSA's central organising principle, yet its vague definition complicates consistent implementation.[18] Co-regulatory mechanisms are potentially powerful instruments to reduce risks, but their effectiveness hinges on clear parameters, measurable indicators, and active enforcement by the EC. Co-regulation

17 Non-compliance with a standard that covers either interfaces (Art. 44[1,i]) to guarantee, e.g., recommender system transparency), or standards for targeted measures to protect minors online (Art. 44[1,j]), theoretically could be linked to non-compliance with risk-mitigation measures that test and adapt VLOPs' algorithmic systems, including recommender systems (Art. 35[1,d]), or take 'targeted measures to protect the rights of the child, including age verification and parent control tools' (Art. 35[1,j]).

18 See also Center for Democracy & Technology, "Civil Society Responds to DSA Risk Assessment Reports: An Initial Feedback Brief", Center for Democracy & Technology, March 17, 2025, accessed October 28, 2025, https://cdt.org/insights/dsa-civil-society-coordination-group-publishes-an-initial-analysis-of-the-major-online-platforms-risks-analysis-reports/ or Dr. Oliver Marsh and Dr. Michele Loi, "A Dual-Track Approach to Systemic Risks under the Digital Services Act", Algorithm Watch, May 5, 2025, accessed October 28, 2025, https://algorithmwatch.org/en/wp-content/uploads/2025/05/250505-Dual-Track-Systemic-Risks.pdf

can contribute to *risk governance* – yet it needs to be effective to do so.

Case Study: How could a crisis protocol work in relation to Art. 35?

To illustrate how crisis protocols could function as a co-regulatory tool for mitigating systemic risks, we can consider a **hypothetical, but realistic, scenario:**

In the context of electoral processes, a coordinated disinformation campaign emerges. Automated networks amplify messages across multiple platforms, fuelling public anxiety and inciting hostility against vulnerable groups. The EC, upon consultation with the Board for Digital Services, determines that the situation constitutes a 'systemic crisis' under Art. 48, posing a serious threat to democratic stability in several Member States. It invites VLOPs and VLOSEs to establish a crisis protocol aimed at mitigating the risk.

Within this framework, the participating platforms could, for instance, agree to:

- Provide real-time data access to vetted researchers, European Digital Media Observatory hubs, national DSCs and the EC to track the spread of harmful narratives
- Launch cross-platform fact-checking collaborations to prevent re-amplification of false claims across services
- Coordinate on the use of AI or inauthentic behaviour (e.g., monitor fake or murky accounts) during electoral processes

In this particular example, the EC has the mandate to initiate a protocol's drafting process, as it constitutes a scenario that requires a rapid, collective and cross-border response. An incentive for platforms to establish a crisis protocol would be, next to political pressure, reputational management and therefore economic reasoning, to demonstrate good faith and compliance efforts, e.g., by tackling a systemic risk, initiating cross-platform collaboration and cooperating with other stakeholders. Plus, platforms would need to show how they meet their DSA obligations on systemic risks otherwise. However, several challenges could occur: First, the EC would need to prove that a) the crisis is 'systemic', b) it has previously consulted with the European Board for Digital Services on the severity of the crisis, c) a concrete time cap was decided on and d) the measures to be taken are strictly limited to what is deemed 'necessary' under Art. 48(4,d). Second, if the EC asked VLOPs and VLOSEs to revise the protocol and/or ask for additional measures to be taken as they are deemed insufficient, platforms cannot be forced to do so, given the protocol's voluntary nature; they could even withdraw at any stage. Yet, noncompliance with the voluntary crisis protocols eventually can lead to sanctions under the risk mitigation framework. Third, the question of who defines what information will be displayed during a crisis, according to Art. 48(2), remains unanswered.

Assessing Impact: Co-Regulation Potentials and Limits

Per se, it is challenging to measure co-regulatory mechanisms' effectiveness in implementing a regulatory regime, given their nonbinding nature. So far, evidence is lacking on whether co-regulatory instruments change platform incentives and behaviours or remain box-ticking exercises for regulators and platforms – mostly because there no structurally applied method to measure their effectiveness exists, and information on their effectiveness has not been included yet in platforms' auditing reports. Second, it is also because the DSA is still a relatively new piece of legislation, and both existing codes of conduct only recently have been integrated fully into the regulation. In contrast, neither crisis protocols nor standards have been used in practice; however, co-regulatory mechanisms have the theoretical potential to enhance the DSA's effectiveness significantly.[19]

Co-Regulatory Mechanisms' Potentials

Flexibility in a fast-changing space and in times of crisis

Co-regulatory instruments enable the EU to respond to platform dynamics without rewriting legislation, i.e., they have the potential to address gaps and flaws in the current legal framework. As for crisis protocols, they enable a quick response during a state of emergency.

Preparedness and foresight

If platforms prepare crisis protocols before a crisis emerges, they may be able to respond more efficiently when a crisis hits. Standards aim at circumventing risks by establishing cross-platform technical standards that allow for comparability.

Narrowing down systemic risks

Co-regulatory mechanisms can promote effective risk mitigation measures in areas that are not adequately addressed by the DSA or in which details still need to be shaped up: For example, due to its soft law nature, codes of conduct can cover or address content that can be regarded as lawful, but awful (e.g., disinformation) but also directly react to emerging or evolving forms of risks. For example, crisis

19 See an extensive overview of potentials here: Rachel Griffin, "Codes of Conduct in the Digital Services Act: Functions, Benefits & Concerns", *Technology and Regulation* (September 2, 2024)

protocols can address crisis situations that were not accounted for directly; however, codes can specify which risks are to be examined and what mitigation measures VLOPs and VLOSEs could take.

Operationalise other DSA obligations

For example, under Art. 39, VLOPs and VLOSEs must create a repository of all ads displayed on their platform. The Code of Conduct on Disinformation provides measures and KPIs for building a repository of political ads, giving VLOPs and VLOSEs some guidance on meeting a DSA standard.

Stakeholder participation

CSOs, researchers and user representatives are to be involved formally in shaping and monitoring co-regulatory instruments, together with platform providers. In theory, this multi-stakeholder approach can develop robust cross-industry frameworks with diverse perspectives, including a fundamental-rights perspective. However, we have observed that civil society engagement remains difficult, if not a checkbox exercise.[20]

Co-Regulatory Mechanisms' Limitations

While co-regulatory mechanisms bear the potential to boost the DSA's effectiveness, the framework itself faces several challenges that may constrain its effectiveness and legitimacy in practice. These challenges are both structural and normative, relating not only to the platforms' own interpretation of reporting obligations, but also underlying assumptions about the relationship between public authority, private actors, and societal accountability. Here are reasons why co-regulatory mechanisms have not been as successful as envisioned so far:

Platform drop-outs

With an increased proximity between the US administration and tech CEOs, and increasing polarisation of DSA enforcement, it is not surprising that platforms opted out of certain commitments to nonbinding obligations before they can be accounted for risk mitigation measures when it is politically savvy and beneficial to withdraw to appease the US administration. For example, platforms that dropped out of commitments under the Code of Conduct on Disinformation could be

20 See Algorithm Watch, " Joint Statement on Stakeholder Inclusion in the Code of Practice on Disinformation Revision Process", Algorithm Watch, February 24, 2022, accessed October 27, 2025, https://algorithmwatch.org/en/code-of-practice-on-disinformation-revision-process/ and L. Gordon Crovitz, "The European Commission's Disinformation Fail", Politico, July 13, 2022, accessed October 27, 2025, https://www.politico.eu/article/european-commission-disinformation-fail/

evaluated by independent auditors on how well they are adhering to commitments they signed – creating an auditing standard that does not take into account the commitments they decided to drop out of, but still could be used to defend platforms' compliance with Art. 45.

Private sector and regulator interests' dominance

Relatively informal multistakeholder participation also may result in big tech companies promoting their shared interests to the disadvantage of other stakeholders. As these processes are to be very inclusive, yet remain rather opaque, they primarily may serve the interests of regulated companies, as well as provide a way for public authorities to influence platform governance under the umbrella of soft law. In the past, we have observed that the EC has set the agenda for which codes are to be drawn, and it still holds the power to determine what constitutes a crisis on the EU level for a crisis protocol to be applicable. With everyone having their own interests, a co-regulatory instrument that balances the interests of every stakeholder involved is difficult to achieve.

Lack of transparency

Existing codes on hate speech and disinformation arguably lacked transparent procedures and inclusive participation. Drafting important soft law instruments before establishing and clarifying the overarching legal framework undermines the possibility for the widest range of stakeholders to participate meaningfully in their development. However, even with the legal framework in place, drafting procedures remain relatively opaque. For example, the EC has stated on its website that it is establishing a special group of experts to work on a Code of Conduct on Age-Appropriate Design, but no further information has been made publicly available on what stage the drafting process is at and whether there have been any updates since 2023.[21]

The European Commission's role

The role of the EC and other stakeholders is not spelled out in all co-regulatory mechanisms: While the EC oversees development and implementation of codes of conduct and crisis protocols by *facilitating* and *encouraging* the drafting process, it has shaped the agenda for what is viewed as urgent and a necessity to be pursued in the form of codes of conduct in the past. This leaves unanswered questions about the development of crisis protocols and standards, e.g., how far does the EC's

21 European Commission, "Special Group on the EU Code of Conduct on Age-Appropriate Design", European Commission, September 20, 2023, accessed October 27, 2025, https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design

encouragement go, and what real opportunity do other stakeholders have in shaping co-regulatory mechanisms? While the DSA provides mechanisms for EC guidance and endorsement, it does not establish an independent oversight body to review the procedural fairness or substantive adequacy of co-regulatory instruments, i.e., the same institution responsible for facilitating co-regulation eventually evaluates its performance.[22]

Questionable impact and mixed outcome evidence

Measuring impacts hinges on platforms' reporting quality, a lack of transparency and limited to no data access (for regulators and researchers): Hate speech removals during monitoring periods improved earlier, then plateaued and eventually declined, while disinformation commitments expanded, yet outcome indicators remain patchy and platform-specific. It can be questioned to what extent codes will produce legitimate outputs, in the sense of meaningful changes in platforms' business practices that put public-interest issues first.

Lessons From Already Existing Codes

Both codes may help provide transparency about the scale and scope of disinformation and illegal hate speech on VLOPs and VLOSEs, but the extent of this transparency requires systematic monitoring of biannual transparency reporting based on self-declarations and annual monitoring exercises conducted by mostly civil society monitors in the case of Code of Conduct.

Case illustrations: Disinformation and election integrity

Code of Conduct on Disinformation

According to a report from Democracy Reporting International (DRI), between 2022 and 2025, during the transition period from a CoP to a CoC under the DSA, platforms reduced the number of measures committed to in the CoP by 31%.[23] While all areas of the Code were affected, the most significant drop-out in commitments occurred in measures supporting the fact-checking community (a 64% decrease), followed by measures on political advertising and research community empowerment. This retreat comes at a critical time, as the U.S.

---

22 See Jan-Ole Harfst, Tobias Mast, and Wolfgang Schulz, "Independence as a Desideratum – DSA Enforcement by the EU Commission," *Verfassungsblog*, July 16, 2025, accessed October 27, 2025, https://verfassungsblog.de/dsa-enforcement-commission/ and Suzanne Vergnolle, "A New European Enforcer? Why the European Commission Should Not Stand Alone in the Enforcement of the Digital Services Act," *Verfassungsblog*, May 23, 2023, accessed October 27, 2025, https://verfassungsblog.de/a-new-european-enforcer/

23 Daniela Alvarado Rincón and Michael Meyer-Resende, "Big Tech Is Backing out of Commitments Countering Disinformation: What's Next for the EU's Code of Practice?", Democracy Reporting International, February 7, 2025, accessed October 24, 2025, https://democracy-reporting.org/en/office/EU/publications/big-tech-is-backing-out-of-commitments-countering-disinformation-whats-next-for-the-eus-code-of-practice

administration pushes for weaker digital regulatory frameworks worldwide – and particularly in the EU. As a consequence, these withdrawals raise critical questions about the Code's long-term viability and ability to achieve its objectives.

An evaluation of VLOPs and VLOSEs compliance and effectiveness conducted by EDMO between January and July 2024 suggests that platforms' efforts to commit to the Code of Conduct remain very limited so far, lacking consistency and meaningful engagement, with initiatives having been criticised as superficial or symbolic. VLOPs and VLOSEs's compliance with the Code's commitments remains inconsistent and impartial across platforms.[24]

This aligns with a review of platforms' code compliance by Mündges and Park, who concluded that many platform responses are not comprehensive, i.e., they leave important aspects or answer reporting obligations by providing only superficial information.[25] Their findings indicate that platforms fall short in fulfilling their reporting obligations. Similarly, the German-Austrian Digital Media Observatory (GADMO) determined there was room for improvement when analysing platforms' self-declarations before the European Parliament elections.[26]

Whether these measures were sufficient will become clearer after the first round of the Code's audit reports, EC feedback on platforms' compliance with the risk mitigation framework and reporting from all relevant stakeholders – including platforms and Code signatories – in the form of self-declaratory transparency reports and risk assessments.

Case illustration: Illegal hate speech

The Code of Conduct + on Combating Illegal Hate Speech

This Code of Conduct used to have far less oversight than the former CoP: Monitoring code compliance has been checked through annual monitoring rounds for a period of a maximum of six weeks, during which a wide range of CSOs is involved. The seventh and last evaluation on the Code of Conduct on Countering Illegal Hate Speech Online (2022) so far reveals that the number of notifications reviewed by signatories within 24 hours (64.4%) decreased compared with 2021 (81%) and 2020 (90.4%).

Drawing on these insights, the DSA's co-regulatory instruments can be evaluated not only in terms of procedural compliance, but also based on their effectiveness in

---

24 European Digital Media Observatory (EDMO), "Implementing the EU Code of Practice on Disinformation: An Evaluation of VLOPSE Compliance and Effectiveness (Jan–Jun 2024)", June 24, 2025, https://edmo.eu/publications/implementing-the-eu-code-of-practice-on-disinformation-an-evaluation-of-vlopse-compliance-and-effectiveness-jan-jun-2024/

25 Stephan Mündges and Kirsty Park, "But Did They Really? Platforms' Compliance with the Code of Practice on Disinformation in Review," *Internet Policy Review* 13, no. 3 (July 25, 2024), pp. 1–21, https://policyreview.info/articles/analysis/platforms-compliance-code-of-practice-on-disinformation-review

26 German-Austrian Digital Media Observatory (GADMO), "CoP Monitor 2024: Strengthened Measures by Major Platforms Are Insufficient During Election Campaigns", November 2024, https://gadmo.eu/wp-content/uploads/2024/11/Report2024_CoP.pdf

mitigating systemic online risks.

Lessons From Other Co-Regulatory Frameworks: Comparing the DSA, GDPR and AI Act

The co-regulatory model institutionalised in the DSA exemplifies a broader shift in the EU's digital regulatory strategy towards a balance between hard law and soft, participatory mechanisms. This evolution reflects the EU's recognition that in fast-moving technological domains, regulation often lacks the agility required for effective oversight. Earlier frameworks, such as the GDPR, embody a similar logic, but operationalise co-regulation through distinct institutional designs. The GDPR's codes of conduct (Articles 40-41) empower industry and professional associations to develop sector-specific compliance standards subject to review and approval by public supervisory authorities. This model preserves strong regulatory hierarchy and rights-based guarantees while allowing for contextual adaptation: The GDPR clearly situates codes as secondary instruments vis-à-vis the GDPR as the primary instrument. Codes are 'intended to contribute to the proper application' of the GDPR (Article 40[1] GDPR) and have 'the purpose of specifying' its application (Article 40 [2] GDPR).

In contrast, the Code of Practice for General Purpose AI (GPAI), a tool to comply with the EU AI Act's GPAI, guides providers of GPAI models in meeting their obligations under the AI Act, developed by independent experts and shaped by stakeholders from industry, academia, CSOs and rightsholders under EC oversight. It is meant to prepare providers for what is ahead and offers a straightforward way to start complying with future obligations under the AI Act. Positioned between these two frameworks, the DSA adopts a deliberative and participatory approach: Its standards, codes of conduct and crisis protocols are mostly multi-stakeholder in nature, engaging platforms, regulators, and civil society in ongoing, risk-based governance.

	GDPR	AI Act	DSA
Legal Basis	Art. 40, 41 GDPR	Art. 56, 57, 95 AI Act	Art. 45, 46, 47, 48 DSA
Function	Compliance tool: allow sectors or associations to translate GDPR principles into practical rules	Transitional and complementary tool: precursor or specification of obligations for GPAI providers, particularly until	Co-regulatory tool: complements legally binding obligations for

		detailed implementing acts take effect	VLOPs/VLOSEs
Binding nature	Voluntary, but can become binding once approved by supervisory authorities or the European Data Protection Board (EDPB)	Semi-binding: voluntary, but key to demonstrating due diligence and compliance under the AI Act; may later become binding via an implementing act	Voluntary, but can be used to demonstrate compliance with Articles 45–48 DSA
Development & Oversight	Drafted by associations or sectors and approved by national data protection authorities (DPAs) and EDPB	Developed by GPAI providers in coordination with the EC, AI Office and AI Board	Developed by platform providers and/or other signatories and coordinated by the EC
Enforcement	Breaches may lead to withdrawal of approval or DPA enforcement actions	No direct sanctions yet, but linked to Articles 53–55 of the AI Act; can influence compliance assessments by supervisory authorities	No direct sanctions, but noncompliance may be viewed as a lack of due diligence under the DSA

Unlike the GDPR, whose co-regulatory instruments are integrated tightly into an enforceable system of rights and remedies, the DSA's mechanisms rely heavily on voluntary commitments. This flexibility enhances adaptability and responsiveness to emergent online risks – particularly in domains such as disinformation and crisis response – but also risks creating accountability gaps. Similarly, for the Code of Practice on GPAI, it remains unclear whether the EC will require full adoption of the Code or allow selective adherence. The DSA opens a procedural space for stakeholder deliberation, yet lacks robust criteria for assessing the effectiveness or inclusiveness of resulting co-regulatory instruments. Taken together, the enduring challenge across all instruments remains the same: ensuring that such procedural flexibility translates into genuine accountability.

How To Make Co-Regulation Work in Practice

While the DSA's co-regulatory framework represents an innovative step towards participatory and adaptive digital governance, several structural and normative challenges threaten its long-term effectiveness. The first concerns the persistent risk of regulatory capture. As large platforms are often the best-resourced participants in drafting co-regulatory instruments, their influence can shape these mechanisms in ways that prioritise feasibility over public interest. Civil society actors, smaller platforms, and independent researchers frequently lack the institutional capacity, resources, or access to influence co-regulatory processes meaningfully. This

imbalance risks reproducing the very asymmetries of power the DSA seeks to correct, raising questions about multi-stakeholder arrangements' democratic legitimacy and representativeness.

A second challenge lies in transparency and accountability. Although the DSA mandates audits and encourages transparency, much of the co-regulatory activity – particularly in code negotiation and monitoring – remains opaque to external scrutiny. Unlike formal legislative procedures, co-regulatory initiatives often lack effective monitoring of implementation. This creates a grey zone of governance in which private actors contribute significantly to the development of normative frameworks without being subject to the same accountability standards as public institutions. The question here remains: Can meaningful consequences be imposed on actors who do not respect agreed-upon rules if they are largely responsible for developing and monitoring these rules themselves? The problem is compounded by the EC's dual role as both regulator and enforcer.

A third challenge is uneven enforcement and fragmentation. The absence of precise benchmarks or measurable indicators for evaluating performance of codes of conduct or crisis protocols further weakens the feedback loop between voluntary commitments and hard law.

Finally, a broader tension is present between flexibility and legal certainty. The DSA's reliance on co-regulation allows for responsiveness to new risks, but it also creates uncertainty about thresholds for compliance and the consequences of noncompliance. This reliance on soft law and voluntary measures may reduce incentives for platforms to engage meaningfully, particularly when the link to enforcement remains weak.

The DSA's success as a regulatory model will depend on its ability to institutionalise accountability without sacrificing flexibility. This may require strengthening mechanisms for stakeholder participation, transparent monitoring, and an informed independent evaluation of co-regulatory mechanisms as outlined in the following section:

Soft law should be nonbinding but properly assessed

In a democratic system like the EU, soft law should serve as a complement, not a substitute for enforceable regulation. Voluntary, nonbinding measures alone, given platforms' lack of consistency, data, and meaningful engagement in code commitments, are unlikely to change platform behaviour and business models' structures that contribute to some of the potential risks associated with VLOPs and VLOSEs. Therefore, co-regulatory mechanisms need proper monitoring and compliance assessment. Without stronger assessment, their implementation risks remaining performative rather than impactful.

A comprehensive monitoring framework ensures effective oversight

Co-regulatory instruments can help develop stronger accountability through concrete commitments, success metrics, impact evaluations and reporting standards – all of which facilitate oversight by regulators, auditors and external stakeholders, and allow for easier industry compliance and comparisons between platforms over time. However, it remains unclear how accountability will be measured effectively. Will compliance be monitored through audits, risk assessments, transparency reporting, code-specific monitoring exercises or all four? Given the extensive scope of the involved tasks and the required planning and allocation of resources, a detailed plan to guarantee harmonised assessment methods – including staff and financial resources – of codes and future crisis protocols should be devised.

Civil society should participate actively, not only symbolically

While the EC's stated aim for development of codes of conduct was to involve various actors, the actual process fell short – and in favour of industry players writing their own rules. Civil society engagement should not be regarded as a checkbox exercise. Including civil society as an effective early-warning system, as envisioned in both codes of conduct, is a first step in the right direction and should be integrated into crisis protocols. The rapid response mechanisms under the Code of Conduct on Disinformation could serve as a successful example here.

Audits need to have a clear framework executed by experts

Effective compliance assessment is the centrepiece of the DSA's ability to regulate online platforms because audits are an essential part of the process, as they assess the effectiveness of platforms' adherence to co-regulatory instruments. Furthermore, platforms' behaviour is currently not held to any external standard. The DSA grants platforms considerable flexibility to define their own benchmarks for audit assessments. However, in the absence of clear guidance from the EC, no consistent way to evaluate the quality of these audits exists currently. As a consequence, these audits need a clear audit framework applied by experts who understand the complexities of systemic risks and platform systems and who can determine how impact can be assessed.

Audits should take the level of commitment into account

With an independent auditing framework comes the responsibility to assess platforms' compliance with Article 45, even if they have withdrawn from certain voluntary commitments (e.g., Code of Conduct on Disinformation). This framework should evaluate platforms against the level of commitments they continue to uphold, ensuring consistent accountability and preventing selective withdrawal from obligations to evade transparency or responsibility.

Codes of Conduct can be used as a best practice for risk mitigation

Beyond its prospective legal enforceability through audits, codes of conduct could operate effectively as a practical best practice for assessing the adequacy of VLOPs and VLOSEs' risk assessments and mitigation measures regarding the topic covered by the codes. Analysing audits of codes of conduct to see what has and has not worked could serve as a basis for best practices reported on in risk assessments under Art. 35(2,b). Using codes as best practices would facilitate a more consistent approach to addressing systemic risks covered by codes.

Rapid response protocols can ensure preparedness

In their risk assessments, many VLOPs and VLOSEs referenced rapid-response protocols in times of crises. Platforms could develop and use these protocols as a baseline to respond swiftly to crises, aligned with DSA Article 48 and existing EU crisis frameworks. They also could share best practices with other platforms, national DSCs and the EC, and directly link these protocols to early-warning systems used in both codes.

Independent monitoring and tangible indicators are needed

With codes of conduct and crisis protocols being subject to audits, analysis of platforms' compliance with their commitments is more crucial than ever. The EC should require platforms to provide clear and comprehensive reports on both qualitative and quantitative KPIs that not only report on measures taken, but also on these measures' impact. Continued independent monitoring is crucial, as well as setting out clear and tangible structural indicators in all codes under Art. 45-47.

Conclusion

So far, evidence is still lacking on whether co-regulatory instruments change platform incentives and behaviours or remain box-ticking exercises for regulators and platforms – also because the DSA is still a relatively new piece of legislation. This paper shows that it is challenging to measure co-regulatory mechanisms' effectiveness in implementing a regulatory regime, given their nonbinding nature.

The DSA tries to circumvent this risk by weaving co-regulation into a system of due diligence, risk assessment, and reporting duties. This means compliance is not left entirely up to the industry. Instead, platforms operate within a publicly monitored framework that still allows for self-regulation. The model helps keep the DSA flexible enough to meet (and regulate) the tech industry where it is, while strengthening legitimacy by involving a range of stakeholders. Without clear benchmarks for assessing how platforms perform, however, soft law mechanisms'

effectiveness can erode easily.

The way forward requires a shift in thinking about co-regulations' role in enforcing regulations they are tied to. Co-regulation need not be in vain, but it requires clearer and more consistent monitoring and assessment to avoid ending up merely symbolic. If the DSA's co-regulatory mechanisms can deliver measurable risk reduction, genuine transparency and equal participation, they may be an effective tool in digital governance. Intensive research would be needed at the appropriate time to assess whether the co-regulatory instruments are fulfilling their purpose.

As the EU is still experimenting with a mix of hard and soft regulation, the DSA is also something of an important test case for co-regulation. It will show whether the Commission's "voluntary, but somehow still binding" approach ends up being effective - and could therefore also serve as a model for other policy areas. Given this very reason, it might also still be too early to evaluate the success and failure of these instruments. The challenge ahead is to ensure that co-regulation as a governance model stays true to its non-binding nature but does not remain without teeth.

Acknowledgements

I would like to warmly thank the experts who were interviewed in the framework of this research, as well as those who kindly agreed to review drafts and provide feedback. Their input greatly contributed to informing and improving this paper. The views expressed here, however, do not necessarily reflect their own or those of their employers.

Special thanks to:

- **Rachel GRIFFIN,** PhD Candidate and Lecturer in Law, *Science Po Paris*
- **Julia Christina HESS,** Senior Policy Researcher, Global Chip Dynamics, *interface*
- **Dr. Julian JAURSCH,** Policy Advisor, *German Digital Services Coordinator*
- **Daniela ALVARADO RINCÓN,** Policy Officer, *Democracy Reporting International*
- **Luisa SEELING,** Lead Writing, Editing & Publishing, *interface*
- **Lisa SODER,** Senior Policy Researcher/ Acting Head Technical AI Governance, *interface*
- **Jacob VAN DE KERKHOF,** PhD Candidate and Lecturer in Law, *Utrecht University of Law*
- **Carl VAN DER MAELEN**, Legal Officer, *European Commission DG CNECT (Communications Networks, Content and Technology)*
- **Dr. Teresa WEIKMANN,** Postdoctoral Researcher, *Amsterdam School of Communication Research/ BENEDMO project*

I would also like to express my appreciation to **ALINA SIEBERT**, Lead Design &

Visual Communication, and **IANA PERVAZOVA**, Lead Media Relations & Outreach at *interface*, for your invaluable visual design and dissemination efforts.

Author

Lena-Maria Böswald
Senior Policy Researcher Digital Public Sphere
lboeswald@interface-eu.org

Imprint

interface – Tech analysis and policy ideas for Europe
(formerly Stiftung Neue Verantwortung)

W www.interface-eu.org
E info@interface-eu.org
T +49 (0) 30 81 45 03 78 80
F +49 (0) 30 81 45 03 78 97

interface – Tech analysis and policy ideas for Europe e.V.
c/o Publix
Hermannstraße 90
D-12051 Berlin

Design by Make Studio
www.make.studio
Code by Convoy
www.convoyinteractive.com