DOT Europe

Streamlining the EU Digital Rulebook

APRIL 2025

FRESHFIELDS | DOT. europe Digital • Online • Tech

Background

For companies doing business in the EU, the potential of the single market promising regulatory stability, sophisticated oversight and access to consumers remains one of the Union's major draws. In recent years however, as digital services and business models have proliferated, the EU's regulatory and legislative response has been piecemeal and to some extent uncoordinated. With the wave of new legislation adopted during the 2019-2024 mandate – but by no means only – digital businesses are increasingly struggling to comply with a patchwork of rules that feature conflicting provisions, duplication of requirements, redundant procedural steps and complex oversight architectures at both the EU and national level.

Companies in the digital sector experience the cumulative effect of these factors which lead to serious consequences, for example the inability to scale across the single market, the chilling effect on innovation due to uncertainty of applicable legal regimes, and the diversion of resources to compliance and legal away from core business streams to name a few. With the recent announcements in the European Commission's 2025 work programme, and the clear target to achieve at least 25% reduction in administrative burdens for companies by the end of this mandate, the scheduled fitness check on the legislative acquis in the digital policy area in particular provides an opportunity to remedy some of these issues.

> The renewed political focus on European competitiveness calls for a thorough and honest review of the EU's digital rulebook. In recent years, the regulatory framework for digital services has expanded significantly – now is the time to clarify overlaps and streamline obligations while maintaining the original regulatory goals.
>
> **Constantin Gissler, Director General, DOT Europe**

This report is not intended to cover the entirety of the EU's vast digital rulebook. Rather, the report focuses on a subset of legislative texts of most relevance to DOT Europe members, in order to identify in a clear, concrete and practical manner, the ways in which the legislative architecture in the consumer and digital spheres can be rationalised, streamlined and refined.[1] The goal is to maintain the policy ambitions of the EU digital rulebook while enabling companies to apply the laws in a way that is simpler, more cost efficient and more effective overall. This report identifies several areas that should and can be addressed through targeted changes, and that if implemented, will have a material beneficial impact on companies doing business in the EU.

The policy recommendations put forward in this report are designed to provide EU policymakers with immediate and actionable remedies, backed up with evidence and examples. The recommendations provided can also serve as signposts and indicators of best practice for future policy deliverables going forward.

> In our practice, we observe that many digital businesses face significant challenges in implementing the various, often overlapping and sometimes contradicting EU regulations. The high administrative burden often reduces capacity to focus on the actual substantive requirements that truly add value for customers in the EU. Simplifying these regulations and reducing unnecessary friction is crucial, as it is key to enabling businesses to operate more efficiently and effectively, ultimately benefiting users of digital services.
>
> **Christoph Werkmeister, Partner, Freshfields**

1 Artificial Intelligence Act (AI Act); Audio-Visual Media Services Directive (AVMSD); Child Sexual Abuse Material (CSAM); Copyright Directive; Cyber Resilience Act (CRA); Data Act; Digital Services Act (DSA); EU Electronic Communications Code (EECC); ePrivacy Directive; General Data Protection Regulation (GDPR); Network Information Security (NIS2); Platform to Business Regulation (P2B); Unfair Commercial Practices Directive (UCPD); Unfair Contract Terms Directive (UCTD).

1.

Structure and methodology

Structure and methodology

This report, commissioned by DOT Europe on behalf of its members, is structured into three pillars: summary table of identified challenges and proposed solutions; in-depth legal analysis of the challenges faced by companies when complying with the EU digital rulebook; and actionable and concrete policy recommendations to address the identified challenges.

The intention of this report is not to be exhaustive in listing all of the challenges faced by companies active in the digital ecosystem, but rather to help focus the attention of policymakers on the most burdensome and common regulatory barriers that are preventing companies from reaping the full benefits of the single market.

The solutions proposed range from targeted legislative amendments, suggestions as to the working practices of the EU institutions as well as proposals for new initiatives (legislative and non-legislative), aligning as much as possible with the deliverables the European Commission has committed to in its 2025 work programme. These should be read as suggestions and will, in some instances, require additional analysis before a fleshed-out solution can be found.

The report is supported by the feedback of DOT Europe's members, having provided their input via a questionnaire and resulting in the identification of the following eight focus areas:

I. Governance structure

II. Documentation requirements

III. Incident reporting requirements

IV. Data access and data processing requirements

V. Content moderation requirements

VI. Transparency requirements

VII. Design of digital services and products

VIII. Best practice for future policymaking and legislating

2.

Summary of identified challenges and proposed solutions

Challenges and solutions

Issue	Solutions
Governance structure Overlap of competences between different regulatory authorities, resulting in interaction by companies with multiple authorities in relation to the same activity. Potential conflicts in relation to the approach that needs to be followed under a new legislative initiative due to spread of competences for digital issues across several departments within the European Commission. Overall lack of common statutory goals between authorities such as competitiveness, innovation, or growth.	• Institutionalise pre-implementation dialogues in the Council. • Ensure companies are not subject to multiple investigations into the same practices / behaviours by different regulators through implementation of appropriate coordination mechanisms. • Introduce common statutory duties for all regulators and the European Commission to have regard to the impact of regulation and enforcement on competitiveness, innovation, and growth.
Documentation requirements Numerous (partly overlapping) documentation requirements, including risk or impact assessments, leading to significant administrative burden for companies and giving rise to higher compliance risks and operational challenges.	• Develop European Commission guidelines on documentation requirements in relation to risk assessments. • Consider whether synergies are possible between various risk assessment duties. For example, consider how to align any risk assessment on child sexual abuse with the risk assessment under Article 34 DSA. • Streamline cybersecurity and technical documentation requirements between the GDPR, CRA and NIS2, e.g. by clarifying that documentation produced for the purposes of one piece of legislation can also be integrated in existing documentation prepared for compliance with another piece of legislation. • Consider reducing the rigidity of independent audit requirements under Article 37 DSA by changing the assurance standard in the delegated act.

Issue	Solutions
Incident reporting requirements Multiple reporting obligations for example under the GDPR, the ePrivacy Directive, the EECC and the NIS2 Directive (and the respective national implementation) with tight reporting deadlines that may apply to the same incident, involving various regulators, requiring different reporting forms, and often requiring distinct types of information.	• Establish a centralised alert mechanism for companies to notify incidents to a single reporting platform. • Develop a single incident reporting mechanism template.
Data access and data processing requirements Numerous data access obligations, in some instances concerning the same types of data, with different requirements in terms of technical approach and exemptions. In addition, various regulatory initiatives at EU level, national laws and local regulatory interpretations as well as overlaps between the GDPR, ePrivacy Directive, the DSA, the Data Act and the AI Act, contributing to the fragmentation of data processing requirements, despite the GDPR's unified approach.	• Streamline data access and data sharing requirements under the GDPR and Data Act to ensure coherence regarding the applicable legal grounds for refusing data access requests. • Produce European Commission guidelines on the interplay between the AI Act and the GDPR. • Modernise the ePrivacy framework by aligning it more closely to the GDPR, in particular with regard to applicable legal bases, before formulating any new legislation impacting this area. • Produce EDPB guidelines to further assist data exporters in their compliance efforts in relation to the Schrems II requirements. • Finalise work by the European Commission on standard contractual clauses. • Increase cooperation with international partners on facilitating data flows on the basis of model contractual clauses.

Challenges and solutions

Issue	Solutions
Content moderation requirements Overlaps in content moderation regulation, particularly regarding the requirement for expeditious action in removing or addressing content. Legal uncertainty despite the fulfilment of commitments under the DSA Codes of Conduct.	▪ Streamline the concept of urgency in the reviews of the DSA and the Copyright Directive. ▪ Produce European Commission guidelines on "notice and action" under the DSA and the Copyright Directive. ▪ Ensure the upcoming guidelines on the application of Article 35(1) of the DSA confirm that the fulfilment of commitments under the DSA Codes of Conduct constitute a presumption for compliance with the DSA content moderation requirements.
Transparency requirements Various transparency requirements with different forms and level of detail for information, resulting in users being confronted with too much information that they cannot digest.	▪ Streamline transparency requirements via an Omnibus simplification package for the digital sector. ▪ Delete requirements under the P2B Regulation on transparency and consider the overall added value of the Regulation. ▪ Significantly reduce and consolidate as far as possible the number and frequency of transparency reports that companies must prepare. ▪ Delete the requirement under the EECC for a contract summary to be provided to consumers. ▪ Review the DSA reporting template via amendments to the relevant implementing act to remove fields that are not required by regulation.
Design of digital services and products Numerous requirements related to the design of digital services and products, in particular aspects concerning the protection of minors and dark patterns, resulting in a fragmented framework and creating legal uncertainty. Fragmentation in respect of contractual requirements introduces further complexity for governance of contractual relationships with business users.	▪ Establish a uniform approach for protection of minors by developing guidelines on the interplay between the DSA and the AVMSD. ▪ Fully enforce existing legislation in relation to B2C dark patterns and only consider targeted changes to existing legislation if gaps are identified.

Issue	Solutions
Best practice for future policymaking and legislating	• Codify the digital rulebook to work towards consistency, prevent further legal overlaps and provide clarity in terms of the hierarchy of legislation. • Create a digital implementation 'Project Group' within the European Commission. • Ensure that any impact assessment prepared for a new legislative initiative gives specific consideration to the impact it would have on the regulatory governance structure established by existing legislation. • Provide for an inter-service consultation among European Commission departments (DGs) before interinstitutional negotiations begin.

3.

Legal analysis

I. Governance structure

The EU digital rulebook introduces a broad set of regulations governing various aspects of the digital economy, including data protection, data access, cybersecurity, and digital services. As a result, offering digital services in the European Union has become a highly regulated activity as this generally entails the application of:

- the General Data Protection Regulation (***GDPR***) and the ePrivacy Directive and its Member State implementation (for the processing of personal data and regarding accessing data on devices);
- the Cyber Resilience Act (***CRA***) (for software products);
- the AI Act (for any AI component in the software and service);
- the Digital Services Act (***DSA***) (to the extent that the service is considered an online platform or search engine);
- the Network Information Security Directive (***NIS2***) and respective Member State implementation (for certain cloud services);
- the European Electronic Communications Code (***EECC***) and respective Member State implementation (for certain communication services);
- the Data Act (in the context of connected devices and for certain cloud services); and
- applicable EU consumer protection rules, including Member State implementation.

Whilst it is not the intention of this report to cover the entire waterfront of legislation applicable to the digital sector, in addition to the above, there are also several other pieces of applicable law, depending on the type of digital service offered. Digital regulation is overseen by various regulators on the EU and Member State level, all of which can – to a certain extent – review user interfaces, backend processing operations, relationships with sub-contractors, data security and public disclosures of the regulated digital services.

While the EU digital rulebook is intended to create a harmonised digital environment within the EU, one significant challenge that businesses face is the overlap of competences between different regulatory authorities. Maintaining a regulatory dialogue and responding to queries regarding new products or developments with such a large array of regulators constitutes a particular challenge for companies. Such companies, active in the digital space, generally operate across borders whilst offering their products in most (if not all) EU Member States. In practice, this means that businesses are often required to interact with multiple authorities in relation to the same activity, each of which may be focused on a different aspect of compliance. For example:

The **processing of special categories of personal data** for the purpose of ensuring bias detection and correction in relation to high-risk AI systems pursuant to Article 10(5) of the AI Act falls within the competence of the competent authority under the AI Act but also of the supervisory authority under the GDPR as it relates to the processing of personal data. Taking Germany as an example, the Federal Network Agency (Bundesnetzagentur) will likely be established as the competent market surveillance authority under the AI Act, whereas compliance with the GDPR is monitored by various data protection supervisory authorities. This means that the same processing activity could be subject to the monitoring of compliance and enforcement of two regulators. A similar situation with different authorities responsible for the enforcement of the AI Act and the GDPR will likely exist in Spain[1], Lithuania[2] and Italy[3].

1 In Spain, the Agencia Española de Protección de Datos (*AEPD*) is the competent authority responsible for enforcing the GDPR, whereas the Spanish Artificial Intelligence Supervisory Agency (*AESIA*) will be established as the market surveillance authority under the AI Act. The notifying body has not been designated yet.

2 In Lithuania, the State Data Protection Inspectorate (*Valstybinė duomenų apsaugos inspekcija*) is the competent supervisory authority responsible for enforcing the GDPR. Under the AI Act, the Innovation Agency will likely act as the notifying authority and the Regulatory Communications Authority as the market surveillance authority.

3 In Italy, the Garante per la protezione dei dati personaliis the competent authority responsible for enforcing the GDPR, whereas under the AI Act, the National Cybersecurity Agency (Agenzia per la Cybersicurezza Nazionale, *ACN*) will likely be designated as the market surveillance authority and the Agency for Digital Italy (Agenzia per l'Italia Digitale, *AgID*) will be designated as the notifying authority.

Similarly, **cybersecurity measures** under the Cyber Resilience Act (***CRA***) include, inter alia, measures for products with digital elements, including ones which process personal data (Article 7(2)(b) CRA), which are also subject to security requirements under the GDPR. Again, this means that different authorities may be competent to review the same type of processing activity, with each regulator focusing on inherently similar regulatory requirements.

Furthermore, the spread of competences for digital issues across several Directorates General (***DGs***) within the European Commission sometimes gives rise to conflicts in relation to the approach that needs to be followed under a new legislative initiative.

Typically, the responsible DG requests the formal opinion of other DGs with a legitimate interest in a new legislative initiative prior to its publication via the inter-service consultation process. However, further dialogue and cooperation among DGs at particular moments of the legislative process would certainly improve the quality and coherence of legislation. Since the only official consultation between Commission services is carried out before an initiative is published, amendments introduced by co-legislators later in the process and that fall outside of the area of expertise of the leading DG often go unnoticed. This creates **contradictions and overlaps especially between horizontal pieces of legislation and sectoral ones**.

The AI Act for example was amended with respect to financial services provisions addressing the potential inclusion of some traditional statistical techniques within the scope of the definition of "AI systems". Due to limited involvement by certain DGs with particular sectoral expertise during the negotiations, further clarification work had to be carried out in Level II legislation (i.e. guidelines on the definition of AI systems) to ensure legal clarity. Such situations leave market participants unsure for prolonged periods of time about whether requirements are indeed applicable to them.

II. Documentation requirements (including risk or impact assessments)

Numerous documentation requirements foreseen in the EU digital rulebook result in a significant administrative burden for companies in preparing, collecting, and retaining the relevant information. Overlapping documentation requirements are also associated with greater compliance risk (e.g. the risk of creating inconsistent documentation) and operational challenges (e.g. in keeping information up to date and accurate across the various sets of documents prepared for different purposes or for different regulators). Documentation requirements may now be disproportionate to the risks they were intended to address. Examples of overlapping documentation requirements include the following:

Both the GDPR and the AI Act require **risk assessments**, with the GDPR focusing on the risks to the rights and freedoms of the data subject associated with a particular processing and the measures implemented by the controller to address those risks (Article 35 GDPR). The AI Act, on the other hand, requires that providers of high-risk AI systems identify, assess, and document the known and reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights, as well as the measures implemented to mitigate respective risks (Article 9(2) AI Act). To the extent personal data is processed in the context of the use of high-risk AI systems, providers have to produce documentation under both the GDPR and the AI Act, with overlapping elements that need to be included in both pieces of documentation.

Additionally, providers of very large online platforms (**VLOPs**) and of very large online search engines (**VLOSEs**) subject to the DSA are required to assess **systemic risks stemming from the design or functioning of their service**, including with regard to potential negative effects on fundamental rights, in particular to the protection of personal data and to non-discrimination (Article 34 DSA). These elements partly overlap with documentation requirements under the GDPR and the AI Act.

A similar overlap resulting in duplicative risk considerations is likely to exist in the context of the proposed Child Sexual Abuse Material Regulation (***CSAM***) and the DSA. The proposed CSAM Regulation also considers imposing a requirement on providers of hosting services and providers of interpersonal communications services to carry out a **risk assessment concerning the use of their services for the purpose of online child sexual abuse** (Article 3 CSAM Proposal). The scope of the risk assessment under the proposed CSAM Regulation overlaps with the scope of the risk assessment under Article 34 DSA, which captures risks of the dissemination of illegal content (including child sexual abuse material) and foreseeable negative effects for the exercise of fundamental rights, including for the rights of the child enshrined in Article 24 of the Charter.

Overlaps also exist with regard to **technical documentation**, e.g. Annex VII of the CRA sets out detailed requirements for documentation for products with digital elements, while at the same time the technical and organisational requirements of respective data processing activities must be documented under Articles 32 and 5(2) GDPR. Similar requirements apply under the AI Act, which also foresees technical documentation requirements for high-risk AI systems that shall be drawn up and kept up-to date, including a general description of the AI system and its intended purpose (Article 11 AI Act). There are various other regulations with specific, but overlapping documentation requirements, for example the Medical Device Regulation (***MDR***) which requires that manufacturers of medical devices draw up and keep up to date technical documentation for relevant devices to demonstrate the conformity of those devices with the requirements set out in the Medical Device Regulation (Article 10(4) MDR). This includes information about how the device works, its intended purpose and intended users. All these overlapping documentation requirements create a significant administrative burden.

There are also overlapping documentation requirements concerning **cybersecurity risks**, including under the CRA (Article 13(2) CRA) and the NIS2 Directive (Article 21 NIS2 Directive), which overlap with documentation requirements under the GDPR, where potential risks to the security of processing and respective measures implemented by the controller need to be documented in order to comply with the accountability principle under Article 5(2) GDPR.

The DSA includes a very detailed and rigid framework for **independent audits** under Article 37 DSA, including with regard to the individual elements to be included in the audit report (Article 37(4) DSA), which includes a description of the specific elements audited, and the methodology applied. While Article 37 DSA aims to ensure that VLOPs or VLOSEs are transparent, accountable, and in compliance with the DSA's consumer protection and content moderation provisions, it also creates a significant administrative burden. This burden is challenging, in particular in light of the various overlapping risk assessment and documentation requirements that need to be fulfilled alongside the independent audit requirements.

III. Incident reporting requirements

The EU digital rulebook imposes multiple reporting obligations that, depending on the circumstances of the individual case, may apply to the same incident, involving various regulators. Each regulator requires different reporting forms, often requesting distinct types of information. The compliance burden is further intensified by the fact that reporting deadlines for incidents are consistently tight, necessitating substantial resources to gather and submit the required information on time.

The NIS2 Directive requires that essential and important entities report **"significant incidents"**, without undue delay, to the Computer Security Incident Response Team or, where applicable, the competent authority (Article 23 NIS2 Directive). It foresees a staggered approach for the information to be provided to the relevant authority, i.e. an early warning within 24 hours of becoming aware of the significant incident, an incident notification within 72 hours after becoming aware of the significant incident, and a final report not later than one month after the submission of the incident notification. The CRA foresees similar reporting obligations for **"severe incidents"**, subject to similar reporting deadlines, to the Computer Security

Incident Response Team and to the European Union Agency for Cybersecurity (Article 14 CRA). Both the NIS2 Directive and the CRA also include ad hoc reporting requirements (Article 23(4)(c) NIS2 Directive and Article 14(6) CRA).

The same incident, to the extent it concerns **personal data**, can be subject to the GDPR, in which case it must be reported to the competent Data Protection Supervisory Authority in accordance with Article 33 GDPR, without undue delay and in any event within 72 hours. Other reporting obligations can apply under the ePrivacy Directive if the data breach occurs in connection with the provision of publicly available electronic communications services (Article 4(3) ePrivacy Directive), in which case the incident must be reported, without undue delay, to the competent national authority, or under the EECC, which requires the reporting of **"security incidents with significant impact on the operation of networks or services"**, without undue delay and in any event within 24 hours, to the competent national authority (e.g. the Bundesnetzagentur in Germany, or Autorité de Régulation des Communications Électroniques, des Postes et de la Distribution de la Presse in France).

The administrative burden is intensified in situations where companies can arguably not rely on one-stop-shop mechanisms (e.g. under the AI Act and under the EECC and ePrivacy Directive or NIS2 Directive) so that filings need to be made to authorities in various Member States, requiring different notification forms and processes, including different language requirements.

In addition to incident reporting obligations, providers of hosting services are subject to obligations to promptly notify law enforcement authorities of instances in which they become aware of information indicating criminal offences involving a threat to the life or safety of a person (Article 18 DSA), whereas under the proposed CSAM Regulation[4], providers of hosting services and providers of interpersonal communication services will be required to promptly report to the EU Centre online child sexual abuse on their services (Article 12 of the CSAM proposal) – which in certain instances can also require reporting of the same facts to multiple authorities.

IV. Data access and data processing requirements

While the GDPR provides a unified framework for data protection across the EU, there are various regulatory initiatives at EU level as well as national laws and local regulatory interpretations that contribute to the fragmentation of data access and data processing requirements. Examples of fragmentation in this space include:

At EU level, **different requirements for the processing of special categories of personal data** are introduced by the GDPR and the AI Act. While the GDPR foresees stringent requirements for the processing of special categories of personal data, with limited grounds to process such data without consent (Article 9 GDPR), the AI Act allows exceptions for processing special categories of personal data for the purpose of ensuring bias detection and correction in relation to the high-risk AI system, provided that certain conditions are met, as stipulated in Article 10(5) AI Act.

The ePrivacy Directive, which imposes stringent **data processing requirements for electronic communications services** (Articles 5(1), 6 and 9 ePrivacy Directive) and for accessing and storing data on devices (Article 5(3) ePrivacy Directive), dates back to an era dominated by traditional telephone services. These rules do not fully account for new communication channels such as instant messaging apps, voice-over-IP solutions, and social media platforms. Furthermore, in practice, the ePrivacy requirements generally overlap with the GDPR. Nevertheless, regulators in EU Member States have enforced the ePrivacy Directive on a local level, despite GDPR lead supervisory authorities based in other jurisdictions. The proposal for an updated ePrivacy Regulation was recently withdrawn, which means that the currently incoherent ePrivacy framework remains in place.

4 Recent Proposal for the CSAM Regulation, as suggested by the Polish Presidency.

Another example concerns data processing activities that fall under the EU Digital Markets Act (***DMA***), triggering a consent requirement, thereby imposing **stricter conditions for the processing of personal data** than the GDPR which foresees six different legal bases for the processing of personal data (Article 6(1) GDPR).

Another example concerns **data transfer requirements** under the GDPR (Article 44 et seq. GDPR), which have been subject to intense debate and scrutiny by the European Court of Justice, most recently in the Schrems II decision.[5] These rules continue to create legal uncertainty, on the one hand in relation to data transfers to the US and most recently regarding data transfers to China.[6] The European General Court even held that not even the European Commission would be able to fully comply with these complex and constantly evolving rules.[7] The Data Act now introduces similar requirements for non-personal data (Article 32 Data Act), thus creating additional legal uncertainty and also deviating from the known concepts under the GDPR. Given that international data processing operations are vital for any global business, in particular in the digital space, the lack of clarification of the EU data transfer regime risks increasing costs for digital services in the EU due to data localisation of server infrastructure or resulting in certain services simply not being provided in the EU.

Finally, **data access and data sharing obligations** in EU legislation, in particular under the GDPR and the Data Act, vary significantly from one another in terms of the technical requirements and the conditions under which data must be made available, or can be withheld by the relevant companies. By way of example, a business that offers connected products or related services in the EU will be subject to the Data Act. At the same time, it can be subject to the GDPR, to the extent the data processed in the context of the connected product or the related service is personal data. As a result, businesses falling under both regimes will have to comply with data access requirements under both the GDPR and the Data Act, which may require different approaches with regard to the same set of data.

Specifically, compliance with both regimes may require different approaches from a technical perspective, given that the Data Act requires data holders to make product and related service data accessible to the user (and third parties) continuously and in real-time where relevant and technically feasible (Article 4(1) Data Act). In contrast, the GDPR requires a mere one-off access to personal data (Article 15 GDPR). Additionally, it remains unclear whether the exceptions for data access included in the GDPR (i.e. where access would result in adverse effects to third-party rights, for example intellectual property rights and trade secrets, and security-related restrictions), are also applicable in the context of data access under the Data Act. The Data Act only specifies requirements for refusal to protect trade secrets, leaving unclear the legal grounds for refusal of data access requests. The lack of clarity increases the compliance burden for relevant businesses in areas that have a direct impact on the product design of digital services.

Furthermore, since the data access obligations in the Data Act are without prejudice to the GDPR (Recital 7 Data Act), the restrictions for processing and sharing personal data under the GDPR have to be taken into account before providing data access to third parties (cf. Article 4(12) Data Act). The main practical issue in this context is the separation of non-personal data from personal data, as many data sets contain both. In practice, this separation will often require disproportionate effort or might even be unfeasible.

As a result of the overlapping data access obligations, businesses will often have to create different data access options for users for the same data set, or have different approaches for different data sets, depending on the data regime that applies. This not only creates major compliance challenges

5 Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems.

6 C093-05 Tencent International Service Europe B.V. | noyb.eu.

7 Judgment of the General Court of 8 January 2025, Thomas Bindl v European Commission.

and requires significant resources and investments, but might also be overwhelming for the user who is confronted with many different data access options. This could lead to confusion and increase the overall complexity of data access request processes, thereby also worsening the overall user experience.

V. Content moderation requirements

Existing EU rules that address content moderation and platform responsibilities create further conflicting requirements, particularly regarding the requirement for expeditious action in removing or addressing content.

Under Article 16, the DSA provides a "notice and action" mechanism where platforms are expected to **remove or disable access to illegal content without undue delay** once they receive a notice. The regulation does not specify an exact timeframe within which the content must be removed, leaving some flexibility in interpreting what constitutes an "undue delay." The expectation is that platforms should act swiftly but also fairly, ensuring that content removal is justified and that users' rights to challenge the removal are preserved. In contrast, Article 17(4)(c) of the Copyright Directive requires an **"expeditious" action to remove infringing content**, upon receiving a sufficiently substantiated notice from the rightsholders. The term "expeditious" also implies quick action but may suggest a stronger emphasis on immediacy and less flexibility compared to the DSA's "undue delay." The difference in urgency between "undue delay" and "expeditious action" can create uncertainty for businesses trying to comply with both regulations. While both require timely removal of content, the Copyright Directive could be interpreted as demanding even quicker action than the DSA, potentially conflicting with the DSA's broader focus on ensuring fairness and the opportunity for users to appeal content removals.

Legal uncertainty in the field of content moderation is further increased by Codes of Conduct (***CoCs***) endorsed under the DSA. Despite their voluntary status (Article 45(1) DSA), the European Commission considers the fulfilment of the commitments of such Codes of Conduct as a **means for VLOPs and VLOSEs to demonstrate compliance** with their obligation to implement reasonable, proportionate and effective risk mitigation measures (Article 35 (1) DSA).[8] Nonetheless, the European Commission also emphasises that adherence to such obligations does not constitute a presumption for compliance with the DSA[9], creating legal ambiguity regarding compliance expectations.

VI. Transparency requirements

A central issue in the digital regulatory landscape is the amount of transparency requirements, often to the detriment of users, who are provided with different types of information in different levels of detail, in different formats, at different points in time, and in varying contexts. The legislative purpose of providing users with more transparency is effectively defeated by providing users with too much information and in formats that they cannot digest.

By way of example, under the GDPR, businesses processing personal data in the context of their services offered in the EU are required to inform data subjects, amongst other things, of the scope and purposes of the processing of their data, and their rights concerning the processing of their data (Articles 13, 14 GDPR). The relevant information shall be provided at the time when personal data is obtained and is usually included in **privacy policies**.

Another example includes transparency requirements under Article 102 EECC which apply to providers of electronic communications services. These include a requirement for certain **pre-contractual information** to be provided to consumers in a clear and comprehensible manner on a durable medium or, where provision on a durable medium is not feasible, in an easily downloadable document (Article 102(1) EECC). This detailed information further specified in Annex VIII of the EECC

8 European Commission, 13.2.2025, C(2025) 1008 final, Commission Opinion on the assessment of the Code of Practice on Disinformation within the meaning of Article 45 of Regulation 2022/2065, para. 8.

9 ibid, para. 17.

shall be accompanied by a concise and easily readable **contract summary**, identifying the main elements of the information requirements mentioned above (Article 102(3) EECC). While the intention of the requirement to publish a contract summary is to increase transparency and help consumers make informed choices, it also comes with a risk of over-simplification and the risk of consumers being overwhelmed with an additional layer of information.

Detailed information requirements are also included in the DSA, where relevant platforms and services are required to disclose information in their **terms and conditions** on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review, as well as the rules of procedure of their internal complaint handling system (Article 14 DSA). Some of the elements to be included in terms and conditions pursuant to Article 14 DSA overlap with the transparency requirements under the GDPR, e.g. the description of procedures used for content moderation, to the extent these involve the processing of personal data, or the existence of algorithmic decision-making, which must also be disclosed to data subjects under the GDPR (Article 13(2)(f) GDPR). Hence, in these instances, users would be presented with the same type of information in terms and conditions and general privacy information. Information concerning the use of recommender systems shall also be set out in the terms and conditions of providers of online platforms (Article 27 DSA), which may partly overlap with information included in privacy policies under the GDPR – e.g. to the extent personal data are used in the context of recommender systems, the provider will need to disclose which type of data is used for the relevant processing, which may overlap with the "criteria" used to determine the information suggested to the user, to be disclosed to the user under the DSA.

While general information on the use of personal data for advertising purposes will typically be included in a privacy policy, for compliance with the GDPR, the DSA introduces additional transparency requirements in relation to advertising measures of VLOPs or of VLOSEs. Article 39 DSA requires in this respect that a **repository of certain information** be included in a specific section of the online interface, through a searchable and reliable tool that allows multicriteria queries and through application programming interfaces.

Under the Data Act, the seller, rentor or lessor, which may be the manufacturer, of a connected product and the provider of related services are required to provide certain information to the user before concluding a contract with the user (Article 3(2), (3) Data Act). This **pre-contractural information** partly overlaps with the information that the relevant companies in scope of the Data Act must already provide to users under Articles 13 and 14 GDPR (to the extent personal data is concerned), e.g. how the users may access, retrieve or, where relevant, erase their data (Article 3(2)(d) Data Act, Article 13(2)(b) GDPR). Similar transparency requirements are also included in relation to cloud services under Article 26 Data Act, which overlap with Article 13(2)(b) GDPR, though requiring more detailed information concerning a user's data portability rights.

Providers of digital services are required to publish several reports under the DSA, relevant Code of Conducts, and the interim derogation from the ePrivacy Directive[10] to be able to detect child sexual abuse online, and under the proposed CSAM Regulation. By way of example, intermediary services must publish a **transparency report** (at least once a year for non-very large online platforms and at least once every six months for VLOPs/VLOSEs) on any content moderation they engaged in during the relevant period (Article 15 DSA and Articles 24 and 42 DSA, as applicable). Additionally, information on the average monthly active recipients of the service in the EU, shall be included at least once every six months in a publicly available section of their online interface. Additional reporting

10 Regulation on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online.

requirements are included in the voluntary EU Code of Practice on Disinformation (related to reporting under Articles 15, 24, 42 DSA), the Regulation on Terrorist Content Online (Articles 5(5), 7(2)), the voluntary Hate Speech Code of Conduct (related to Article 35(1)(c) DSA) and under the Child Sexual Abuse Material Interim Regulation (Article 3(1)). Similar transparency reporting requirements are also considered under the proposed CSAM Regulation (Article 84 of the CSAM Proposal).

In the context of the processing of customer data in financial services, the proposed Financial Data Access Regulation (FiDA) mandates that data holders in scope of the proposed regulation provide certain information to customers, through a **permission dashboard**, providing an overview of access and use of their data (Article 8 FiDA).

Other transparency requirements occur in the context of the Platform to Business (***P2B***) Regulation, with the focus on **transparency vis-à-vis the business users** of online intermediation services, requiring providers of such services, amongst other things, to disclose in their general terms and conditions the parameters determining ranking of goods and services, and the possibility to influence ranking against any direct or indirect remuneration (Article 5 P2B Regulation).

Further, under the Audiovisual Media Services Directive (***AVMSD***), Member States are obliged to ensure that media service providers provide easy, direct and permanent **access to certain information** (inter alia their name, geographical address of establishment, contact details) **to the recipients of a service** (Article 5 AVMSD).

VII. Design of digital services and products

The EU digital rulebook also contains numerous requirements related to the design of products and services, including vis-à-vis minors, resulting in a fragmented framework and creating legal uncertainty. The same applies with regard to contractual terms and practices, which are similarly subject to a fragmented legal framework.

There is a significant overlap between the AVMSD and the DSA in their objectives to ensure the protection of users (especially minors).

Under the DSA, providers of online platforms accessible to minors shall, amongst other things, implement **appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors on their service** (Article 28(1) DSA), and shall not present advertisements on their interface based on profiling in instances in which they are aware with reasonable certainty that the recipient of the service is a minor (Article 28(2) DSA). These rules are currently complemented by those set out in Article 28b AVMSD, which also aim to **protect minors on video-sharing platforms**. It is currently unclear as to whether there is even room for Member States to create national implementations of the requirements of the AVMSD, in light of the fact that the DSA aims to *exhaustively* regulate minors' protection on online platforms.

Several legal frameworks include provisions to protect users against **dark patterns** and manipulative design practices, such as the DSA (Article 25), the Unfair Commercial Practices Directive (Articles 6 et seq.), the P2B Regulation (Articles 3 and 5) as well as the AI Act (Article 5). Additionally, the GDPR applies in instances in which specific techniques are used to obtain consent from data users, potentially interfering with the requirement of consent to be freely given (Recital 32 GDPR). Moreover, the European Commission has announced plans for a Digital Fairness Act, which could further overlap with existing requirements addressing dark patterns. Although the legislator has provided some guidance on the interplay between the different provisions (e.g. Article 25(2) DSA stipulates that Article 25(1) DSA shall not apply to practices covered by the Unfair Commercial Practices Directive and the GDPR), businesses nevertheless face legal ambiguity and compliance challenges in light of the fragmented requirements concerning similar types of techniques in different contexts.

While the **use of general terms and conditions** for consumer purchases of goods and services from traders are regulated by the Unfair Contract Terms Directive (***UCTD***), there are

various additional provisions that affect the lawfulness and enforceability of contractual terms. For example, in business-to-business relations, data holders are obliged to agree on fair, reasonable and non-discriminatory terms and conditions for data access with third parties to whom the data holder is required to provide data access under the Data Act (Article 8(1) Data Act). Similar requirements have been introduced under the DMA in relation to conditions of access of business users to software application stores, online search engines and online social networking services (Article 6(12) DMA). A potential future Digital Fairness Act will likely introduce further provisions in this regard which will increase the complexity and the interplay between the various provisions.

4.

Policy recommendations for the identified issues and challenges

The legal analysis set out several conflicting provisions, duplication of requirements, redundant procedural steps and complex oversight architectures, grouped into seven distinct sections. Based on these, the section that follows, sets out a series of concrete policy recommendations and actions to help remedy the identified challenges. The main goal of this section is to identify options that can be implemented by policymakers to streamline and rationalise applicable legislative requirements for companies doing business in the EU. The net result of these actions whether taken individually or combined, will contribute to reducing the existing administrative burden that arises from the EU's digital rulebook, allowing companies to continue growing, competing and offering innovative services, products and solutions to EU consumers while safeguarding their rights.

Most of the policy recommendations outlined here have been conceived with as much alignment as possible to the upcoming policy deliverables of the European Commission, for example, the upcoming fitness check on the legislative acquis in digital policy. In addition, a wide array of legislative and non-legislative options has been put forward depending on the nature of the challenge in question. Lastly, some of the policy recommendations suggested are oriented towards institutional changes or targeting the decision-making and policymaking mechanisms of the EU institutions.

I. Governance structure

In order to guarantee the coherent enforcement of the EU's digital rulebook and reduce administrative burden for companies needing to interact with multiple regulatory authorities when developing new products and complying with EU legislation, the following solutions are proposed:

- Institutionalise **pre-implementation** dialogues among Member States to ensure supervisory convergence. Following up on the ad hoc practice established by the Polish Presidency for the AI Act, Council Presidencies should facilitate pre-implementation dialogues to ensure consistency in the interpretation of key provisions of new legislative acts to streamline implementation and enforcement at the national level. These dialogues would take place between Member State attachés in the Council and would for example look at national experiences and precedents, best practice and identification of common questions.
- The European Commission should explore **mechanisms to ensure that within and between EU Member States, companies are not subject to multiple investigations** into the same practices/behaviours by different regulators. Alternatively and as a minimum, the Commission should include provisions taking inspiration from the Data Act, stipulating that a competent authority can exercise its competence only if the individual company is not subject to enforcement proceedings under the Data Act regarding the same facts by another competent authority (Article 37(13) Data Act), with the ability of the leading authority to request assistance from a competent authority in another Member State (Article 27(15) Data Act). This would significantly ease the administrative burden on companies as well as on regulators who may be unwittingly duplicating efforts of others, while retaining the ability to feed into the lead regulator's work.
- Further efficiency gains could be achieved through better coordination between the European Data Protection Board (***EDPB***) and national Data Protection Authorities (***DPA***s) as well as increased harmonisation of the guidance they issue.

II. Documentation requirements

The policy recommendations aimed at streamlining overlapping documentation requirements affect pieces of legislation that have already been passed and are subject to review according to the European Commission's 2025 Work Programme, as well as legislation under implementation, and initiatives that are currently under negotiation.

Based on the European Commission's plans for 2025 and the state of play of the CSAM Regulation, the following recommendations should be considered to reduce administrative burden on companies:

- Develop European Commission **guidelines on documentation requirements in relation to risk assessments** under the framework of the GDPR, the AI Act, the DSA and the CSAM Regulation to clarify overlaps. The goal of this non-binding tool would be to help companies combat the existing overlaps between risk assessments required under the GDPR (Article 35) and for high-risk AI systems under the AI Act (Article 9(2)). In addition, the guidelines should include a section on the partial overlap between risk assessments under the GDPR, the AI Act and Article 34 of the DSA to unify the wording of these requirements and allow companies compliant with the documentation requirements outlined in one of these three texts, to be exempt from providing additional risk assessments.
- Broader consideration should be given to identifying where possible **synergies between various risk assessment duties**. For example, once interinstitutional negotiations begin on the CSAM Regulation, the European Commission should consider how to align any risk assessment on child sexual abuse with the risk assessment under Article 34 DSA which also captures risks of the dissemination of illegal content. This can be achieved by clarifying in the legal text that the more specific risk assessments under the CSAM regime can be integrated into the more general risk assessment under the DSA.
- **Streamlining cybersecurity and technical documentation requirements** between the GDPR (Article 5(2)), CRA (Article 13(2)) and NIS2 Directive (Article 21) should be tackled as part of the upcoming **digital package** to avoid duplications and minimise additional burdens. This could be achieved by adding a clarification that providers should have a choice on whether to integrate the required information and documentation into documentation and procedures that already exist under other pieces of legislation, similar to the approach taken under the AI Act (Article 8(2)).
- Consider reducing the rigidity of Article 37 DSA on independent audit requirements by changing the assurance standard in the relevant Delegated Act.

III. Incident reporting requirements

Significant administrative burden is placed on companies for the purposes of reporting incidents, and in particular those offering their services across several EU Member States – sometimes needing to file multiple reports within 24-72 hours and often in different languages. As outlined in the legal analysis, this administrative burden is intensified in situations where companies are unable to rely on one-stop-shop mechanisms. To remedy this, the following recommendations are proposed:

- Establish a centralised alert mechanism allowing companies to **notify incidents to a single reporting platform** as currently under discussion in the Council. A single entry point for incident reporting has the potential to significantly reduce administrative burden for companies while increasing the efficiency with which incidents are dealt with, as well as alleviating pressure on competent authorities.
- Develop a **single incident reporting mechanism template** to enable providers to file a single notification to all authorities in order to streamline reporting obligations within feasible deadlines. The template should align the deadlines and definitions (e.g. the definitions of "significant incidents" under NIS2 Directive (Article 23) and "severe incidents" under CRA (Article 14)). Ideally the template would allow providers to file notifications in one language only and would clarify that other parties in the supply chain do not have to notify incidents which occur on a third-party service (e.g. cloud provider). This would alleviate pressure on regulators and avoid them being overloaded with multiple notifications regarding the same incident, thereby focusing their resources on the principal incident.

IV. Data access and data processing requirements

Divergent data access and data sharing obligations under the GDPR, the Data Act and other data access regulation (e.g. the Financial Data Access Regulation) in relation to technical requirements and conditions under which data must be made available or can be withheld by the relevant business, currently results in serious compliance hurdles for companies. Suggestions to tackle this are as follows:

- As part of the upcoming **fitness check of the *digital acquis*** expected by the end of 2025, we encourage the European Commission to identify ways to **streamline data access and data sharing requirements under the GDPR and the Data Act** to ensure coherence regarding the applicable legal grounds for refusing data access requests. The upcoming fitness check should also ensure that restrictions for processing and sharing personal data under the GDPR do not incur unnecessary and disproportionate efforts on companies that are subject to the Data Act when sharing data with third parties.

Despite GDPR providing a unified approach to data processing requirements, other pieces of legislation that have recently been enacted (for example the AI Act), include conflicting provisions for companies. Suggestions to clarify such overlaps and ease the compliance burden for companies are as follows:

- As a follow up to the fitness check of the digital acquis area that is expected to target both the GDPR and the AI Act, the European Commission should develop **guidelines on the interplay between the AI Act and the GDPR**. These guidelines would streamline the stringent requirements for the processing of special categories of personal data with limited grounds to be processed without consent under GDPR (Article 9), and the exceptions provided under the AI Act for the purpose of ensuring bias detection and correction in relation to the high-risk AI system (Article 10(5)), among other issues.
- In order to provide maximum clarity for companies and ensure the least disruption to business operations, the EDPB (as instructed in the European Commission's Second Report on the application of the GDPR[11]), **should explore ways and tools, in particular guidelines, to further assist data exporters in their compliance efforts in relation to the Schrems II requirements**. Furthermore, the European Commission should **finalise the work on additional standard contractual clauses**, in particular for data transfers to data importers whose processing is directly subject to the GDPR (also outlined in the 2024 GDPR report). A further action to undertake is to **increase cooperation with international partners on facilitating data flows on the basis of model contractual clauses**.

V. Content moderation requirements

Content moderation requirements across the DSA and the Copyright Directive are often unharmonised and create legal uncertainty for companies, particularly regarding the requirement for expeditious action in removing or addressing content. As both pieces are subject to a potential review in the current mandate, suggestions to solve these conflicts are outlined below:

- Ensure that the upcoming **reviews of the DSA and the Copyright Directive streamline the concept of urgency** for removing or disabling access to illegal content under the DSA and for infringing content under the Copyright Directive by choosing a harmonised approach between the existing terms (i.e. “undue delay” under Article 16 of the DSA and “expeditious” under Article 17(4)(c) of the Copyright Directive).
- The European Commission should **prepare guidelines on “notice and action” under the DSA and the Copyright Directive** ensuring that requirements for platforms are harmonised and proportionate across these two pieces of legislation, thereby ensuring there is no difference in relation to the concept of “urgency”.

11 Communication from the Commission to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52024DC0357.

- Despite the non-binding nature of the Codes of Conduct, we invite the European Commission and Digital Service Coordinators to indicate in the upcoming **guidelines on the application of Article 35(1) of the DSA**, that fulfilment of the commitments of such Codes of Conduct by VLOPs and VLOSEs constitute a presumption for compliance with the DSA content moderation requirements.

VI. Transparency requirements

Transparency requirements are outlined in different forms and level of detail in numerous pieces of legislation including the GDPR, the DSA and the P2B Regulation, among others. As a result, the initial legislative purpose of providing users with more transparency is sometimes defeated, and leads to users receiving too much information which is difficult to digest.

Set out below are the concrete recommendations for EU policymakers to consider while trying to consolidate existing transparency requirements in a cohesive manner:

- Inclusion of a **dedicated chapter on "transparency requirements"** under a potential upcoming **Omnibus simplification package for the digital sector**. This chapter would streamline the existing overlap between some of the elements included in the "terms and conditions" pursuant to Article 14 of the DSA with the transparency requirements outlined under the Article 13(2)(f) of the GDPR. In addition, further clarification should be provided in relation to the potential overlap between information concerning the use of recommender systems set out in the "terms and conditions" of providers of online platforms (Article 27 DSA) and the information included in privacy policies under the GDPR.
- **Deletion of the requirement under EECC for a contract summary to be provided to consumers** (Article 102(3) EECC).
- **Deletion of the requirements under the P2B Regulation on transparency** vis-à-vis the *business users* of online intermediation services (Article 5 P2B Regulation) and broader consideration of the added value of this Regulation.
- **Significantly reduce and consolidate as far as possible the number and frequency (ideally no more than once a year) of transparency reports** that companies must prepare, across multiple legislative texts including the DSA, relevant Codes of Conduct and the proposed CSAM Regulation. Additional reporting requirements should also be streamlined across the following texts: EU Code of Practice of Disinformation, Regulation on Terrorist Content Online, Hate Speech Code of Conduct and CSAM Interim Regulation.
- One solution to operationalise the above point would be for the European Commission to **review the DSA reporting template via amendments to the relevant implementing act** to remove fields that are not required by regulation to ensure that this template could be also repurposed for Child Sexual Abuse Material detection.

VII. Design of digital services and products

The fragmented regulatory framework governing consumer protection has led to a vast number of requirements for the governance and design of digital services and products particularly in relation to minors and dark patterns. While the EU's approach until now has been focused on developing further regulation to clarify unclear concepts, the path forward should now be focused on streamlining concepts and avoiding overlaps under upcoming binding and non-binding tools which are in the pipeline. Suggestions to ensure a uniform approach towards consumer protection are as follows:

- Given the current lack of clarity and differences in approach that companies and consumers must navigate, the **consumer protection obligations in the EECC and the UCTD should be streamlined**.
- Noting that the DSA is without prejudice to the AVMSD (Article 2(4)(a)), the European Commission must ensure that upcoming **guidelines on the protection of minors** under Article 28 of the DSA guarantee that the measures in place delivering compliance with the obligation to take appropriate measures to protect minors from videos and audiovisual commercial communications which may impair their physical, mental or moral development (Article 28b AVMSD) also satisfy compliance with Article 28(1) DSA. The guidelines

should clarify the interplay between the abovementioned two provisions and establish a harmonised, proportionate and technology neutral approach that impedes potential overlaps with national measures that could currently be adopted based on Article 28b AVMSD. Given the potential review of the AVMSD by the end of 2026, the aspects outlined above should be considered to guarantee further harmonisation and ensure that national bills do not overlap with the DSA.

- The presence or not of any gaps in the regulation of B2C dark patterns, despite the myriad of existing rules already covering them, requires further assessment. The immediate priority should be the **correct and full enforcement of existing legislation**. Only when a gap or evidence of a failure in the acquis is identified, should further regulation be considered (also against the need for increased simplification). In addition, the benefits of potential new initiatives should be carefully weighed against the downside of further increases in the complexity of the applicable rules.

VIII. Best practice for future policymaking and legislating

This report identifies several overlaps and conflicting provisions within the existing digital rulebook and especially between horizontal and sectoral pieces of legislation. With the aim of ensuring that companies operating in the digital sector are able to operate under a stable and predictable legal framework and environment, the following actions could be considered to increase institutional coordination and improve the quality of future policymaking:

- **Codification of the digital rulebook** should be undertaken by the European Commission. The purpose of the codification would be to set out the applicable provisions of the digital rulebook for companies whilst also providing clarity in terms of the hierarchy of legislation (for example the instances where *lex specialis* applies and the relationship between different provisions with similar requirements). Codification would also have the benefit of providing a tool for EU legislators to be able to verify in a "pre-emptive" manner, potential overlaps, duplication and redundancies across existing and upcoming new laws affecting companies operating in the digital sphere.
- Create a **digital implementation Project Group**. This group would bring together all the European Commission departments responsible for the implementation of digital legislation. European Commission 'Project Groups' have already been set up to ensure coordination between the various European Commission services on topical issues (without prejudice to the decision-making process), which should be expanded to also include a grouping on "digital implementation". This new Project Group should be led by DG CNECT, with involvement from other relevant departments including DG JUST, DG FISMA, DG SANTE and DG GROW, among others. The Project Group's first focus area should be the upcoming fitness check of the digital acquis as well as the digital package, and potential Omnibus simplification package for the digital sector that may come in 2026. The Project Group would align on a common position as to the aims and content of these deliverables, giving particular consideration to avoiding potential overlaps, conflicts and inconsistencies.
- Ensure that any **impact assessment** drafted by the European Commission ahead of the preparation of a new legislative initiatives includes a **dedicated section on regulatory governance**. The purpose would be to ensure that legislators do not add unnecessary regulatory governance structures that further overlap and over-complicate the enforcement and implementation of the digital rulebook both for companies and regulators. For example, assessing whether the creation of a new enforcement body or agency at national level is essential, whether its tasks are already carried out by another body but from a different perspective or for a different purpose, and whether the tasks assigned to it are already undertaken by an existing body at national or European level.
- Provide for an **inter-service consultation** among European Commission departments with a legitimate interest in a given legislative initiative before interinstitutional negotiations begin. Once the European Parliament and the Council reach

their respective positions ahead of trilogues, a two-week inter-service consultation should be run to allow departments to flag any potential overlaps or other inconsistencies and challenges that might arise from the amendments tabled by the co-legislators. As a result, the European Commission should formulate a single position that can be taken into the trilogue negotiations that would limit to the extent possible any potential overlaps and inconsistencies before the text is finalised.

February 2025, 498429 | DS 221115

freshfields.com