Brussels, March 2026

BSP Position Paper: Digital Fitness Check

Business & Science Poland

This position paper is submitted on behalf of Business & Science Poland (BSP) *in response to the European Commission's Call for evidence for an evaluation on the "Digital Fitness Check". It addresses the Commission's identified areas of concern with concrete simplification proposals drawn from industry experience.*

Background

Europe's digital regulatory framework has grown rapidly in recent years, with important new rules aimed at strengthening safety, trust, resilience and fairness across the Single Market. While these objectives remain essential, the cumulative effect of overlapping obligations, fragmented enforcement structures, and parallel reporting and transparency duties is creating unnecessary complexity for businesses operating across borders. In many cases, companies must comply with multiple provisions pursuing similar goals under different legal instruments, often under the supervision of different authorities and according to different timelines, definitions and procedures. Such heavy burdens can be handled mainly by the largest enterprises - often from outside the EU - whereas young innovative companies give up on operations in the European market. The EU's regulatory approach often slows innovation, as varying national requirements, overlapping supervisory bodies and excessive implementation ("gold-plating") discourage digital firms from operating across borders. Moreover, restrictions on data storage and processing raise operational costs and limit the creation of large datasets vital for AI development, while differing public procurement rules across Member States further increase the fixed costs faced by cloud service providers.

BSP Position

As the continent looks to capitalize on the AI revolution, we believe that regulatory **simplification** and **coherence should be treated as strategic priorities**. Since 2019, over **100 new EU regulations** have targeted the digital economy, and today, more than 60% of Europe's businesses cite regulation as their primary obstacle to investment. This density can inadvertently create a **fractured landscape** that complicates compliance and slows the scaling of digital services across the Single Market.

BSP calls for action that preserves the EU's high standards while improving coherence, proportionality and legal certainty. The recommendations below seek to streamline

Rue Belliard 40, 1000 Brussels
e-mail: info@zpbsp.com
EU Transparency Register Number: 548212735276-89

existing rules, reduce duplication, and ensure that regulation remains future-proof, innovation-friendly and supportive of Europe's long-term competitiveness.

Key BSP recommendations

- **Make simplification measurable and enforceable**: prioritise the removal of overlapping obligations across the EU digital rulebook (not only procedural changes), with clear hierarchy rules where instruments regulate the same compliance task.
- **Strengthen harmonisation and reduce national fragmentation:** where full harmonisation already exists (or is intended), prevent divergent national implementation and "gold-plating" that recreates fragmentation for cross-border services.
- **Streamline content and platform rules around the DSA where it already fully harmonises**: remove duplicate obligations from older consumer and platform instruments where they pursue the same objective and avoid adding new layers.
- **Transparency reporting duties:** align definitions, metrics, templates and reporting cycles across EU instruments and codes.
- Clarify hierarchy and precedence between overlapping regimes.
- Modernise and de-duplicate ePrivacy/GDPR.
- Update ePrivacy confidentiality rules to match today's services and security needs.
- Create explicit incentives for Privacy-Enhancing Technologies (PETs).
- Introduce mandatory coordination in a multi-regulator environment to reduce conflicting interpretation and enforcement across overlapping EU digital laws.
- Simplify cybersecurity incident reporting and align timelines and triggers.
- Move towards a single reporting mechanism, harmonised thresholds and a 72-hour standard, applying a "report once, comply with many" principle across overlapping requirements.
- Tie compliance timelines to technical readiness.

Detailed Recommendations

Artificial Intelligence

As currently designed, the Act risks fragmenting the single market: its flexible enforcement structure has led one Member State to plan nine different national AI regulators, and if every country followed suit there could be over 240 such authorities, creating an unprecedentedly complex oversight and enforcement system that would overwhelm administrative capacities. Computing thresholds that trigger requirements on AI models should be raised (many current models already exceed the proposed values), with a roadmap to shift toward capability-based criteria in the future. Obligations for model changes should scale with the significance of the change - fine-tuning a model should incur compliance duties only if it materially alters the model's risk profile. These adjustments will ensure the AI Act supports trust and innovation by being more risk-based, proportionate, up-to-date and feasible to implement.

<table>
<tr><td colspan="2">#1 Revise Compute Thresholds for GPAI Models with Systemic Risks</td></tr>
<tr><td colspan="2">Provisions concerned:
The focus is on Article 51(2) of the EU AI Act, which establishes the training compute threshold (currently 10^25 FLOPs) for presuming that a General-Purpose AI (GPAI) model has high-impact capabilities and as such, poses systemic risks (GPAISR).</td></tr>
<tr><td colspan="2">Current situation:
While training compute was an initial quantifiable starting point, it is becoming a less predictive proxy for a model's actual capabilities and associated risks. Advancements in model architectures and techniques such as distillation, quantization, and post-training compute mean that models trained with less compute can now exhibit more risk or higher performance than older, larger models. The resources required to reach the current 10^25 FLOPs level have significantly decreased, making it accessible to a wider range of actors and no longer representative of the true frontier.</td></tr>
<tr><td>Practical Challenge & Business Impact</td><td>Proposed recommendation</td></tr>
<tr><td>Regulatory false positives: A 10^25 FLOPs threshold risks capturing a growing number of models that do not possess unique systemic capabilities, subjecting providers to the most stringent obligations unnecessarily.
Resource misallocation: Over-inclusion dilutes the AI Office's resources, pulling focus away from the most impactful systems and placing an undue compliance burden on SMEs.
Safety gaps: The current metric creates a low-compute loophole where highly capable, efficiently built models may miss the threshold (false negatives), while outdated frontier models are over-regulated.
Lack of future-proofing: A fixed threshold inevitably becomes outdated as hardware and software efficiency gains continue, necessitating frequent and reactive regulatory revisions.
Market distortion: Current thresholds may create disincentives for using highly performant models,</td><td>Lift compute thresholds: Raise the compute thresholds to 10^26 FLOPs for GPAISR models. Raising the threshold better reflects the scale of computation currently associated with frontier models and provides headroom while standard capability evaluations are developed.
Develop a roadmap for a capabilities-based trigger: Use the 10^26 FLOPs threshold as an initial ex-ante flag, but complement it with an agile mechanism to designate models below that threshold as systemic risks if they demonstrate equivalent high-impact capabilities.
International alignment: Collaborate with technical initiatives (e.g., Frontier Model Forum) to develop clear, objective criteria and benchmarks for identifying systemic risks based on models' capabilities rather than just their size.
Regular cadence for review: Commit to revisiting these thresholds regularly (every 12-18 months) to ensure they do not become over-inclusive of non-</td></tr>
</table>

potentially stifling innovation and reducing the availability of advanced models in the EU.	frontier models or under-inclusive of efficient, high-risk systems. **Anchor modification thresholds:** Ensure that modification thresholds are anchored to the base model to maintain consistency and prevent market distortion.

Content and Consumer regulations

This section sets out targeted simplification proposals addressing duplication, overlap and fragmentation across EU content and consumer rules. The provisions below show recurring situations where compliance tasks are regulated in parallel under multiple instruments, including, among others,: the **Digital Services Act (DSA)** alongside the **Consumer Rights Directive (CRD)**, the **Unfair Commercial Practices Directive (UCPD)**, the **Platform-to-Business Regulation (P2B)**, the **e-Commerce Directive (ECD)**, the **Audiovisual Media Services Directive (AVMSD)**, the **Terrorist Content Online Regulation (TCOR)** and the **European Media Freedom Act (EMFA)**. Additional layers arise through the **GDPR**, the **Digital Markets Act (DMA)**, the **AI Act**, **ePrivacy framework**.

The recommendations that follow therefore focus on: (i) removing or narrowing duplicative obligations where fully harmonised DSA requirements already cover the same policy objective; (ii) withdrawing legacy provisions that enable divergent national rules and undermine harmonisation, notably where parallel AVMSD obligations continue to apply to services already in scope of the DSA; (iii) clarifying hierarchy and precedence where regimes overlap; and (iv) streamlining transparency reporting, templates, definitions and timelines across remaining regimes to reduce administrative burden and improve coherence.

#1 **Overlap in recommender system obligations**	
Provisions concerned: Articles 27 & 38 DSA; Article 6a(1) CRD; Article 7(4a) UPCD; Article 5 P2B Regulation	
Current situation: The DSA establishes horizontal transparency obligations for recommender systems, including disclosure of main ranking parameters and the option to choose non-profiling-based recommendations. At the same time, the Consumer Rights Directive (CRD) and the Unfair Commercial Practices Directive (UCPD) require platforms to provide consumers with information on the parameters determining ranking in online interfaces. Furthermore, the Platform-to-Business Regulation (P2B) imposes parallel transparency duties concerning business users.	
Practical Challenge & Business Impact	**Proposed recommendation**
These obligations coexist without clear delineation of scope or hierarchy. Moreover, the convergence	The Commission should remove overlapping recommender system and ranking transparency

of these regulatory requirements - each subject to oversight by different competent authorities - results in a fragmented and complex compliance landscape.	obligations from the CRD and the UCPD, in light of the comprehensive framework established under the DSA for both consumer and business users and should avoid further layering regulation through the Digital Fairness Act (DFA), focusing instead on streamlining and clarifying the current regime
#2 **Redundant and overlapping regulation of Dark Patterns**	
Provisions concerned: Articles 25 DSA; Article 6 et seq. UCPD; Recital 32 GDPR; Article 13 DMA	
Current situation: Dark patterns are regulated under Article 25 of the DSA, the UCPD, the GDPR (in particular Recital 32), and Article 13 of the DMA, each with its own legal basis and enforcement structure.	
Practical Challenge & Business Impact	**Proposed recommendation**
These obligations coexist without clear delineation of scope or hierarchy. Moreover, the convergence of these regulatory requirements - each subject to oversight by different competent authorities - results in a fragmented and complex compliance landscape.	The Commission should remove overlapping recommender system and ranking transparency obligations from the CRD and the UCPD, in light of the comprehensive framework established under the DSA for both consumer and business users and should avoid further layering regulation through the Digital Fairness Act (DFA), focusing instead on streamlining and clarifying the current regime
#3 **Fragmented and overlapping transparency reporting obligations**	
Provisions concerned: Articles 14, 24 & 42 DSA; Article 7 TCOR; Article 11(4) P2B Regulation; Commitment 39 & 40 Disinformation Code; Commitment 3.2 & Annex Illegal Hate Speech Code; Article 3(1)(g)(vii) Interim ePrivacy Regulation; Article 18 EMFA	
Current situation: The DSA requires intermediary service providers to publish detailed content moderation transparency reports (annually, or twice a year for VLOPs/VLOSEs), based on an extensive reporting template. At the same time, providers of various types of intermediary services are subject to a patchwork of additional EU instruments imposing similar but distinct transparency and reporting obligations, each with its own metrics and reporting cycles. For example, Article 7 Terrorist Online Content Regulation (TCOR) requires annual transparency reports on removal orders, compliance rates and the use of automated tools. Article 11(4) of the P2B Regulation mandates annual reporting on the functioning of internal complaint-handling systems. Commitments 39 and 40 of the Code of Conduct on Disinformation require signatories to publish transparency reports, with VLOPs and VLOSEs reporting twice a year. Commitment 3.2 and Annex II of the Code of Conduct on Illegal Hate Speech Online require reporting on measures taken to address illegal hate speech. Article 3(1)(g)(vii) of the temporary ePrivacy Regulation obliges NI-ICS providers using voluntary CSAM detection technologies to publish detailed annual reports, based on an extensive reporting template. Finally, Article 18(8) of the European Media Freedom Act (EMFA) requires VLOPs to disclose annually specific information on restrictions imposed on media service providers' content.	
Practical Challenge & Business Impact	**Proposed recommendation**

The coexistence of these regimes creates legal uncertainty, data inconsistencies and significant administrative burdens. Divergent definitions (e.g. "actioned" versus "removed or restricted" content) complicate data reconciliation and public interpretation, while misaligned reporting cadences further undermine the coherence and comprehensibility of the resulting datasets. Compressed production timelines also place unnecessary pressure on providers when processing, validating and structuring the underlying data, despite this being a complex and resource-intensive task.	Transparency reporting obligations in the content space should be streamlined by relying on the DSA as the central framework. Additional suggestions include: • Standardising Timelines: Align reporting cadences across instruments, allowing at least a two-month publication window after the reporting period ends. • Annualising Reporting: Shift the Code of Conduct on Disinformation reporting to an annual cycle. • Withdrawing Duplicative Reporting: Eliminate the redundant transparency requirements found in the P2B and the TCOR, which the DSA now covers. • Upholding DSA Harmonisation: Issue clear guidance ensuring the DSA's full harmonisation effect prevents Member States from imposing new transparency reporting requirements, specifically via the national implementation of directives such as the Audiovisual Media Services Directive (AVMSD).
#4 **Overlap in risk assessment obligations**	
Provisions concerned: Articles 34 & 35 DSA; DSA Minors Guidelines; Articles 55(1)(b) & 9(2) AI Act; Article 35 GDPR; Article 5(2) TCOR	
Current situation: In addition to Articles 34 and 35 DSA, comparable but non-identical risk assessment and mitigation duties arise under Article 9(2) Artificial Intelligence Act (AI Act), Article 35 GDPR, the DSA Minors Guidelines and Article 5(2) TCOR, often enforced by different regulators (or different departments within a single regulator).	
Practical Challenge & Business Impact	**Proposed recommendation**
This patchwork creates ambiguity, leading to duplicate compliance work and hindering the effective operationalisation of risk management duties.	The Commission should issue clear guidance to harmonise overlapping risk assessment duties, permitting a single assessment to fulfil multiple legal requirements. Additionally, the Commission should exempt VLOPs/VLOSEs from any new or existing content-related risk assessments already covered by Articles 34 and 35 of the DSA.
#5 **Overlap between the DSA Codes of Conduct and binding obligations**	
Provisions concerned: DSA Codes of Conduct (Article 45 DSA); Articles 14, 16, 27 & 40 DSA	
Current situation: The voluntary Codes of Conduct converted into DSA Codes under Article 45 DSA contain commitments that mirror or replicate existing DSA requirements. For example, commitments in the Illegal Hate	

Speech Code overlap with Articles 14 and 16 DSA (terms and conditions and notice-and-action systems). Commitment 19 of the Disinformation Code overlaps with Article 27 DSA (recommender system transparency), while Commitment 27 assigns the vetting of researchers to a third-party body, contrary to Article 40 DSA, which designates Digital Services Coordinators as responsible for vetting.	
Practical Challenge & Business Impact	**Proposed recommendation**
This creates legal uncertainty and imposes additional compliance costs on providers.	The Commission should ensure that Codes of Conduct adopted under Article 45 DSA do not duplicate or overlap with binding DSA obligations. This would reduce legal uncertainty and alleviate the burden of additional compliance costs on providers, who currently need to demonstrate compliance with overlapping requirements repeatedly under independent third-party audits.
#6 **Overlap between content moderation frameworks**	
Provisions concerned: Articles 14-17, 20 & 21 DSA; Article 28b AVMSD	
Current situation: The DSA imposes harmonised obligations on intermediary service providers regarding content moderation, leaving no room for additional national requirements. At the same time, Article 28b AVMSD provides a parallel regulatory framework for content moderation by video-sharing platforms, which also fall within the DSA's scope.	
Practical Challenge & Business Impact	**Proposed recommendation**
With the coexistence of these regimes, Member States continue to adopt stricter or divergent national rules, undermining the DSA's harmonisation objective. This results in regulatory fragmentation and increased compliance complexity for cross-border service providers.	The Commission should consider repealing Article 28b AVMSD, as its requirements have been superseded by the DSA's fully harmonised framework. At a minimum, Article 28b(6) AVMSD should be withdrawn, which allows Member States to impose stricter measures while complying with EU law.
#7 **Overlap in advertising transparency obligations**	
Provisions concerned: Article 26(1) & (2) DSA; Article 6 ECD; Articles 9 & 28(b)(2) AVMSD	
Current situation: Article 26 DSA requires online platforms to ensure that advertising is clearly identifiable and that the advertiser is disclosed, and to provide functionality for users to declare commercial communications. Overlapping identification and transparency requirements exist under Article 6 e-Commerce Directive (ECD) for commercial communications forming part of information society services, and under Articles 28b(2) and 9(1) AVMSD for audiovisual commercial communications on video-sharing platforms. The purpose of these requirements is the same: enabling users to identify advertising and advertisers.	
Practical Challenge & Business Impact	**Proposed recommendation**
The overlaps cause legal uncertainty for providers of online platforms, and increase the risk of fragmented enforcement by the European Commission on the one hand, and Member State authorities on the other.	In light of the full harmonising effect of Article 26 of the DSA, the European Commission should consider exempting online platforms from aspects of Article 6 of the ECD and Article 9(1) of the AVMSD. The Commission should avoid further layering regulation through the DFA, focusing

	instead on streamlining and clarifying the current regime.
#8 **Overlap in contact information obligations**	
Provisions concerned: Article 11 & 12 DSA; Article 5 ECD	
Current situation: Articles 11 and 12 DSA require intermediary service providers to designate and publish single points of contact for authorities and users. Article 12(2) DSA clarifies that these obligations apply in addition to those under the ECD. Article 5 ECD similarly requires service providers to make contact details, including an email address enabling rapid and direct communication, easily and permanently accessible. While the DSA framework is fully harmonised, the ECD provisions remain variably transposed across Member States.	
Practical Challenge & Business Impact	**Proposed recommendation**
The coexistence of these parallel regimes creates duplication and legal fragmentation, undermining the DSA's harmonisation objective and centralised contact structure.	The Commission should consider exempting providers of intermediary services from the application of aspects of Article 5 of the ECD to remove duplication.
#9 **Overlapping Legal Bases for Requesting User Data**	
Provisions concerned: Article 10 DSA; eEvidence Regulation	
Current situation: Article 10 DSA requires intermediary service providers to respond to orders from national judicial or administrative authorities to provide specific information about individual service recipients and to confirm receipt and execution of such orders. At the same time, the eEvidence Regulation establishes a separate, harmonised framework governing cross-border production and preservation orders for electronic evidence in criminal proceedings, covering similar categories of data requests.	
Practical Challenge & Business Impact	**Proposed recommendation**
The coexistence of these regimes risks creating duplicative or overlapping legal bases for requesting user data, leading to uncertainty regarding the applicable procedural safeguards, scope and execution requirements.	The Commission should clarify that the eEvidence Regulation takes precedence over Article 10 DSA, and that Article 10 DSA should not be used by Member State authorities which are subject to the eEvidence Regulation to request information about recipients of the service in the context of criminal investigations.
#10 **Parallel Terms and Conditions Obligations**	
Provisions concerned: Article 14 DSA; Article 3-10 P2B Regulation; Articles 5 & 7 TCOR	
Current situation: Article 14 DSA sets requirements for the terms and conditions (T&C) of intermediary services, including obligations relating to content moderation, algorithmic decision-making, complaint handling and changes to the T&C. In parallel, Articles 3–10 P2B Regulation impose detailed T&C requirements for online intermediation services in their relationship with business users, including notice periods, ranking transparency, suspension grounds and data access. Articles 5 and 7 of the TCOR require hosting service providers to include provisions in their T&C to prevent misuse for terrorist dissemination and to clearly set out their related policies, including the use of automated tools. These regimes may apply concurrently to certain services.	

Practical Challenge & Business Impact	Proposed recommendation
Providers must comply with different layered T&C frameworks, which may apply in parallel to the same service and contractual relationship. This increases drafting complexity, administrative burden when updating terms, and parallel enforcement exposure. The accumulation of mandatory disclosures may also reduce clarity and intelligibility	The Commission should consider clarifying the interaction and hierarchy between Article 14 DSA, the P2B and the TCOR T&C regime, and assess whether certain P2B and TCOR requirements are still required, or could rather be streamlined within the DSA framework. Greater consolidation would improve coherence and legal certainty while maintaining existing protections.
#11 **Parallel Statement of Reasons Obligations**	
Provisions concerned: Article 17 DSA; Article 4 P2B Regulation; Article 11 TCOR; Article 17 EMFA	
Current situation: Article 17 DSA requires hosting providers to issue a statement of reasons (SoR) when restricting content, suspending or terminating accounts, or otherwise limiting access to the service. Article 4 P2B Regulation similarly requires online intermediation services to provide a SoR to business users prior to or when restricting, suspending or terminating their services. Article 11 TCOR requires hosting providers to make available to content providers information on removals and, upon request, to provide a SoR. Article 17 of the EMFA requires providers of VLOPs to communicate to media service providers a SoR prior to suspending the provision of their online intermediation services on the ground that content is incompatible with T&C. For services falling under all these regimes, all sets of obligations may apply to the same decision.	
Practical Challenge & Business Impact	**Proposed recommendation**
The parallel application of these regimes creates uncertainty regarding their interaction, e.g. regarding timing and content requirements. Providers may have to assess a single restriction decision against divergent legal standards, increasing procedural complexity and enforcement exposure.	The Commission should consider clarifying the interaction and hierarchy between these provisions, and assess whether simplification through reliance on the DSA requirement alone would reduce duplication and legal uncertainty while maintaining existing safeguards.
#12 **Parallel Complaint-Handling and Out of Court Dispute Settlement Obligations**	
Provisions concerned: Article 17 DSA; Article 4 P2B Regulation; Article 11 TCOR; Article 17 EMFA	
Current situation: Article 20 DSA requires online platforms to provide an internal complaint-handling system for recipients challenging certain restriction decisions. Article 21 DSA establishes a framework for certified out-of-court dispute settlement bodies. Article 11 P2B Regulation similarly requires providers of online intermediation services to establish an internal complaint-handling system for business users, including specific procedural guarantees. Also, Articles 12 and 13 P2B further require providers to identify mediators for out-of-court settlement of disputes relating to the provision of the service. Article 10 TCOR likewise requires hosting providers, subject to specific measures, to implement an effective complaint mechanism for content removals, including procedural safeguards and reason-giving obligations. In addition, Article 28b AVMSD requires Member States to ensure that VSP providers under their jurisdiction establish complaint procedures. For services that qualify under more than one of these regimes, these complaint and dispute settlement frameworks may apply in parallel.	
Practical Challenge & Business Impact	**Proposed recommendation**

Providers may have to ensure compliance with multiple layered complaint-handling / dispute settlement regimes addressing different user categories and/or subject matter, but often operating within the same service environment. For example, while the DSA establishes a harmonised framework, the AVMSD leaves discretion to Member States as to the detailed design of complaint procedures, leading to divergent national approaches. This increases procedural complexity and administrative burden and legal uncertainty as to whether a single integrated system suffices.	The Commission should consider clarifying the interaction between Articles 20–21 DSA, Articles 11–13 P2B Regulation, Article 10 TCOR and Article 28b AVMSD. It should assess whether greater procedural alignment or consolidation would enhance coherence.
#13 **Reduce requirements for duplicative consumer information**	
Provisions concerned: Article 6 CRD	
Current situation: Article 6 CRD requires traders to provide extensive pre-contractual information to consumers prior to each transaction. In practice, this obligation also applies to repeated transactions with the same provider, including transactions concluded via account-based relationships or AI assistants, even where a framework agreement already governs future purchases and the relevant information remains unchanged.	
Practical Challenge & Business Impact	**Proposed recommendation**
Specifically for account-based transactions where the consumer enters into a framework agreement covering future transactions upon creation of an account, the repetition of most of the information set out in Article 6 CRD seems superfluous as they apply likewise to all transactions.	The Commission should ensure that Article 6 CRD does not require repeated pre-contractual disclosures for recurring or framework-based transactions where the relevant information remains unchanged. Not displaying this type of information increases the attention on the information essential for the consumer when making another transaction: The main characteristics of the goods or services and the price (and, in case of subscriptions, the duration of contract and conditions for terminating). The repetition of all other information is unnecessary because the consumer knows these are laid down in the framework agreement.
#14 **Modernize information requirements**	
Provisions concerned: Article 6 CRD	
Current situation: The CRD requires traders to provide a phone number and email address for pre-contractual contact and to make a standard withdrawal form available for e-commerce purchases.	
Practical Challenge & Business Impact	**Proposed recommendation**
These requirements no longer reflect digital consumer behaviour or market practice, leading to	Real-time chat support is more aligned with what consumers expect and prefer. Therefore the

unnecessary formalities and limited practical value for consumers.	Commission should clarify that real-time chat support may fulfil the CRD's communication requirements.
#15 **Rebalance right of withdrawal for digital services**	
Provisions concerned: Article 14 CRD	
Current situation: For services that cannot be provided completely within a period shorter than 14 days, consumers may consume or "binge" the most valuable content they are interested in within the right of withdrawal period (e.g., over a weekend) and would then only incur the compensation obligation of a very small amount if calculated on a pro-rata basis from the monthly/annual/etc. price of the service (which may be way more costly to calculate and provide than issuing a full refund).	
Practical Challenge & Business Impact	**Proposed recommendation**
The only way to mitigate these risks would be to introduce a rule that access to a digital media subscription service will only be granted 14 days after purchase. However, this would neither be in the interest of the consumer nor the business. This burden seems particularly heavy when it is borne solely out of uncertainty, because an offer cannot be clearly classified as a digital service or digital content due to a lack of sufficient guidance, and in case of doubt, it should be assumed to be a digital service.	The Commission should clarify that the right of withdrawal for digital services may be excluded under conditions equivalent to those for digital content, particularly where the service consists in providing access to digital content.

ePrivacy and GDPR

The proposals in this section therefore focus on modernising and de-duplicating the ePrivacy/GDPR framework in a way that reflects how communications services and data processing work in practice. The recommendations address connected issues: (i) structural incoherence in the telecoms rulebook caused by placing core voice-service and network-operation provisions in the ePrivacy Directive while telecom services and infrastructure are governed by the EECC and the proposed Digital Networks Act (DNA); (ii) a dual compliance regime for traffic and location data. The section also proposes modernisation where current rules do not reflect today's technical realities.

#1 **Modernization of legacy provisions regulating telecommunications**
Provisions concerned: Articles 7, 8, 10, 11 and 12 of the ePrivacy Directive
Current situation: The current regulatory framework has a "split personality": the ePrivacy Directive governs basic telecom functions (like CLI and call forwarding), while the European Electronic Communications Code (EECC) and proposed Digital Networks Act (DNA) covers the telecom services and underlying infrastructure. "Legacy" articles (7, 8, 10, 11, 12) on traditional voice services are tied to the ePrivacy

Directive, which is now focused on web tracking and data privacy. This fragmentation, especially as ePrivacy is modernized, leads to inconsistent application of telecom law across Member States	
Practical Challenge & Business Impact	**Proposed recommendation**
The regulatory split for telecommunications providers creates significant legal uncertainty and administrative overhead due to navigating two distinct national transposition measures (EECC and ePrivacy) with differing definitions. This "double-jeopardy" compliance forces vetting a single service update against both consumer protection and specific technical mandates. The shift to all-IP networks further blurs the line between privacy and service features. This friction hinders cross-border feature rollout and diverts legal resources from innovation and security to reconciling overlapping requirements.	The most logical path is to transfer ePrivacy Directive Articles 7, 8, 10, 11, and 12 (covering itemised billing, CLI presentation/restriction/exceptions, automatic call forwarding, and malicious calls) to the EECC and the proposed DNA reg, both of which have a number of similar provisions. These provisions concern network operation, billing transparency, and consumer voice service choices, making the EECC (and an EECC successor like the DNA) their appropriate home. This consolidation simplifies the ePrivacy Directive, allowing it to focus on communication confidentiality and terminal equipment protection, while improving legal certainty for providers.
#2 **De-duplication of traffic and location rules**	
Provisions concerned: Article 6 and 9 ePrivacy Directive	
Current situation: The ePrivacy Directive was passed before the GDPR and as a result covered traffic and location rules. However, the GDPR, adopted years after the ePrivacy Directive, provides a more appropriate home for these provisions. For example, the GDPR provides a comprehensive, and technologically-neutral framework for the processing of all personal data, including traffic, location, and marketing data. The specific rules in the ePrivacy Directive are now largely redundant and create a confusing dual regime that is difficult to navigate. Article 5(1) is sufficient to regulate confidentiality without the need for additional granular provisions.	
Practical Challenge & Business Impact	**Proposed recommendation**
The primary challenge for European operators is the competitive disadvantage created by this dual-layered compliance. Organizations are forced to maintain two separate legal compliance architectures for the same data sets, leading to increased costs and a chilling effect on R&D within the European telecoms sector.	The European Commission should repeal Articles 6 and 9 of the ePrivacy Directive and transition the protection of traffic and location data entirely into the GDPR framework. By doing so, the horizontal nature of the GDPR would finally apply to the telecoms sector, allowing providers to utilize the full suite of GDPR safeguards e.g., DPIAs while benefiting from the same lawful processing bases available to the rest of the digital economy.
#3 **Extension of data retention period for law enforcement purposes**	
Provisions concerned: Articles 5, 6 and 15(1) ePrivacy Directive and Article 28 of DSA 6 and 9 ePrivacy Directive	
Current situation: Under the ePrivacy Directive (Articles 5 & 6), traffic and communications data must be erased or anonymized once no longer needed for transmission. Article 15(1) allows Member States to retain data for limited periods (often one year by default) for national security or criminal investigations. However,	

the lack of a harmonized EU retention standard means data may be deleted by service providers before authorities request it for complex investigations.	
Practical Challenge & Business Impact	**Proposed recommendation**
The core challenge is the conflict between ePrivacy erasure requirements and the DSA's strict safety obligations (Articles 28, 34, 35) to manage systemic risks like child protection and illegal content. The typical 12-month retention window is insufficient for serious crime investigations (e.g., child sexual exploitation, sophisticated cyber-attacks), as most law enforcement data requests occur after this period. This forces organizations to risk violating ePrivacy rules or failing to provide data essential for prosecuting serious offenses.	The European Commission should formally extend the data retention period for serious crime investigations to (say) 24 months. This retention window must align with the DSA's child protection and systemic risk requirements, providing legal certainty for providers and a sufficient look-back period for authorities, especially to protect children.
#4 **Modernize the principle of confidentiality for a competitive communications environment**	
Provisions concerned: Article 5(1) ePrivacy Directive	
Current situation: Today's hyper-competitive communications landscape offers sophisticated services that rely on automated processing to deliver immense user value. The current ambiguity chills innovation and slows the roll-out of services that benefit end-users everyday (e.g. facilitating writing messages, suggesting responses, searching and organising the messages), but also enables more inclusion for persons with disabilities (e.g. text-to-speech). Furthermore, the current text fails to explicitly recognize that processing to detect and block spam, malware or severe harmful and illegal content is not an invasion of privacy, but an essential and necessary component of providing a safe and usable service.	
Practical Challenge & Business Impact	**Proposed recommendation**
Article 5(1) was drafted for a world of simple voice calls and SMS. Today's hyper-competitive communications landscape offers sophisticated services that rely on automated processing to deliver immense user value. The current ambiguity chills innovation and slows the roll-out of services that benefit end-users everyday (e.g. facilitating writing messages, suggesting responses, searching and organising the messages), but also enables more inclusion for persons with disabilities (e.g. text-to-speech). Furthermore, the current text fails to explicitly recognize that processing to detect and block spam, malware or severe harmful and illegal content is not an invasion of privacy, but an essential and necessary component of providing a safe and usable service.	We propose to modernize the confidentiality principle under Article 5(1) of the ePrivacy Directive by distinguishing between the prohibited act of interception and two legitimate categories of processing: first, providing innovative, automated features that enhance the user's experience; second, employing automated detection tools to protect user security and prevent the dissemination of illegal or severe harmful content (mirroring existing practical exemptions in jurisdictions like the UK); and third, the operation of minor ancillary features, which are not part of the core communication service and should be governed by the GDPR's more flexible, risk-based framework. We also recommend clarifying that stored data falls under the GDPR to remove legal uncertainty as to which regime applies, and ensuring that a robust but more flexible data protection regime applies once a communication is complete,

	thereby aligning the law with both technology and user expectations.
#5 **Right to information about data recipients**	
Provisions concerned: Article 15(1)(c) and Articles 13/14(1)(e) GDPR and Article 11 of the DMA	
Current situation: GDPR (Articles 13-15) and DMA (Article 11) require that users be informed about data recipients. However, the legal trend, supported by recent rulings, mandates providing specific identities rather than categories. For controllers in a complex digital economy, this is technically an almost impossible requirement to meet, and also risks overwhelming users by providing them with lengthy lists of recipients that are not meaningful to them.	
Practical Challenge & Business Impact	**Proposed recommendation**
For large digital service providers, providing a specific, exhaustive list of recipients for every user's data is technically challenging and creates a massive administrative burden due to the dynamic, millisecond-level nature of digital advertising and cloud ecosystems. Presenting hundreds of unrecognizable names could cause information overload, making the right to be informed incomprehensible and meaningless to the average consumer. Furthermore, the risk of omitting a single automated recipient exposes organizations to legal liabilities.	We propose modernizing GDPR Articles 15(1)(c) and 13/14(1)(e) to explicitly include consideration for the "state of the art" and "technical feasibility" when identifying specific data recipients. The Commission should clarify that providing defined categories of recipients is sufficient for transparency when a specific list is technically not feasible, disproportionate or confusing. This approach, harmonized with the DMA, ensures Gatekeepers provide meaningful, "clear and comprehensive" transparency without an impossible standard of perfect mapping of all data recipients, even minor ones.
#6 **PETs Incentives**	
Provisions concerned: Article 25(1) GDPR	
Current situation: Under the GDPR and other new EU digital laws, PETs are currently voluntary and lack formal regulatory weight. Consequently, controllers investing heavily in advanced PETs often face the same regulatory scrutiny during (say) a Legitimate Interests Assessment (LIA) or Data Protection Impact Assessment (DPIA) as those using basic encryption. This lack of regulatory distinction means the significant cost and complexity of PETs deter their use rather than offering a competitive advantage.	
Practical Challenge & Business Impact	**Proposed recommendation**
Organizations do not receive a clear compliance dividend for using PETs, as current legislation doesn't explicitly recognize their use to favor the controller in the Article 6(1)(f) balancing test or other GDPR assessments. This regulatory uncertainty stalls innovation, especially in sensitive sectors like healthcare and finance, preventing data use for things like collaborative AI. The result is a low-uptake trap: PETs are expensive, yet the lack of regulatory incentive prevents the market from maturing, forcing businesses to rely	It is recommended that Article 25 and Article 6(1)(f) of the GDPR be amended to provide explicit incentives for the use of PETs. Specifically, Article 25 should be updated to mandate that controllers have "particular regard" for recognized PETs when determining the state of the art. Crucially, a new sub-paragraph should be added to Article 6(1)(f) stating that when assessing if a controller's legitimate interest overrides a user's rights, regulators must give significant weight to the technical safeguards implemented, specifically

on older, less effective privacy measures to manage legal risk.	mentioning Privacy-Enhancing Technologies. This would create a safe harbor effect where the use of robust PETs provides a stronger legal presumption of compliance, effectively incentivizing the industry to shift toward a privacy-by-default technical architecture.
#7 **Inter-Regulatory Consultation Duty**	
Provisions concerned: Article 25(1) GDPR	
Current situation: The EU's digital landscape features a "multi-regulator" environment where services are subject to multiple overlapping laws (GDPR, AI Act, DSA, Data Act). Despite this, there is no formal requirement for authorities (e.g., DPAs, AI Office) to consult before enforcement or guidance. The Digital Omnibus promotes general cooperation but lacks a mandatory consultation rule, leading to regulatory silos.	
Practical Challenge & Business Impact	**Proposed recommendation**
Lacking a formal cooperation framework, businesses face a fragmented, unpredictable regulatory landscape with conflicting national guidance and enforcement. This legal uncertainty increases compliance costs, particularly for SMEs and startups, hindering innovation and investment. Furthermore, a lack of coordination wastes regulatory resources and risks inconsistent protection of fundamental rights across the EU.	We propose 3 changes: 1. Mandate Inter-Regulatory Consultation: Introduce a statutory duty requiring national authorities to consult relevant regulators when issues span multiple EU digital regulations (e.g., AI Act, GDPR) to ensure consistent enforcement and guidance. 2. Establish a Formal Inter-Authority Forum: Create a structured forum with a clear mandate and regular meetings for enforcers of EU digital laws. This forum should facilitate information sharing, coordination, and policy alignment, particularly where regulations intersect. The Digital Clearinghouse framework warrants consideration. 3. Develop Joint Guidance and Mandate Public Consultations: Authorities must collaboratively develop shared guidelines on key overlaps (e.g., GDPR and AI Act). All guidance from national authorities and EU bodies (including the AI Office, EDPB) must undergo mandatory public consultation.

Security

This section sets out targeted simplification proposals across the EU cybersecurity reporting and compliance landscape, focusing on the interaction between **NIS2**, the **Cyber Resilience Act (CRA)**, and the evolving **Cybersecurity Act (CSA) revision**. The recommendations respond to three recurring problems reflected in the provisions below: (i) incident reporting requirements that are staged, time-compressed, and inconsistent

across frameworks (including parallel "early warning" obligations and differing triggers); (ii) fragmentation created by national transposition choices under **NIS2**, which complicates cross-border compliance and diverts resources away from resilience; and (iii) binding obligations under the **CRA** that depend on definitions, guidance, and harmonised standards that remain under development, creating planning uncertainty against fixed enforcement dates. The section also addresses how the CSA revision could strengthen a secure-by-design approach by enabling earlier, systematic assessment of cybersecurity impacts across EU policymaking, rather than treating security as an add-on during implementation.

<table>
<tr><td colspan="2">#1 Incident reporting process under NIS2</td></tr>
<tr><td colspan="2">Provisions concerned:
Article 23(4)(a) and 23(4)(b) NIS2 Directive and Recital 102 NIS2 Directive.</td></tr>
<tr><td colspan="2">Current situation:
The NIS2 Directive requires a multiple-stage incident reporting process. Under Article 23(4), essential and important entities must submit an "early warning" to the computer security incident response team (CSIRT) or competent authority within a strict 24-hour window of becoming aware of a significant incident, which must then be followed by a more detailed incident notification within 72 hours. This adds to a highly complex and fragmented landscape of EU regulatory regimes—such as the CRA, DORA, and the AI Act—that mandate incident reporting under different criteria and to different authorities. Notably, the GDPR already establishes a standard that a data breach must be reported to the relevant supervisory authority within 72 hours of discovery if it is likely to imperil individuals' rights and freedoms.</td></tr>
<tr><td>Practical Challenge & Business Impact</td><td>Proposed recommendation</td></tr>
<tr><td>These duplicative, dissonant, and aggressive reporting requirements create an enormous administrative burden. A 24-hour early warning deadline forces organizations to divert highly specialized, scarce incident response personnel away from crucial active threat investigation, containment, and mitigation efforts. While the NIS2 Directive states in Recital 102 that early warnings should only include necessary information and should not divert resources from incident handling, the reality is that instead of focusing purely on resolving the active incident, security teams must scramble to notify various regulators across potentially 27 EU Member States. This premature 24-hour reporting mandate ultimately hinders, rather than helps, the overarching goal of rapid and effective incident response.</td><td>Amend NIS2 Article 23(4)(a) and consolidate it with Article 23(4)(b) to revise and standardize initial incident reporting timelines across NIS2 and other frameworks around a 72-hour deadline. Aligning with the existing GDPR 72-hour standard promotes consistency and reduces the overlapping compliance burdens placed on scarce incident response personnel, allowing them to prioritize mitigating the threat before filing formal notifications</td></tr>
<tr><td colspan="2">#2 NIS2 framework for a high common level of cybersecurity across the Union</td></tr>
<tr><td colspan="2">Provisions concerned:
NIS2 Directive</td></tr>
</table>

Current situation: The current legal framework for a high common level of cybersecurity across the Union is established as a Directive (the NIS2 Directive (EU) 2022/2555). While NIS2 aims to address the inherent shortcomings of its predecessor (NIS1) by setting out minimum rules for a coordinated regulatory framework, it still requires transposition into national law by all 27 Member States by October 17, 2024, which has been considerably late in many Member States. As a Directive, it inherently leaves considerable discretion to individual Member States regarding its exact implementation.	
Practical Challenge & Business Impact	**Proposed recommendation**
Relying on a Directive rather than a directly applicable instrument preserves regulatory fragmentation within the internal market. As the NIS2 text itself acknowledges, disparities in national rules "entail additional costs and create difficulties for entities that offer goods or services across borders," and conflicting requirements "may substantially affect such cross-border activities". Multinational organizations are forced to build complex, 27-jurisdiction compliance matrices to manage differing national transpositions of incident reporting thresholds, supervisory measures, and legal liability. This patchwork approach diverts vital security resources away from actual cyber resilience and into localized administrative compliance. Furthermore, leaving execution to national discretion means that the "inadequate design or implementation of cybersecurity requirements in one Member State is likely to have repercussions at the level of cybersecurity of other Member States," creating vulnerabilities with spill-over effects across the Union.	Transition the overarching cybersecurity framework from a Directive to a single, directly applicable EU Regulation. Unlike a Directive, a Regulation automatically and uniformly applies across all Member States without relying on 27 individual national transposition laws. Adopting a Regulation would establish a truly harmonized baseline for cybersecurity risk-management measures and reporting obligations, eliminating the "wide divergences among Member States" that lead to internal market fragmentation. This structural shift would provide absolute legal certainty, eliminate overlapping and conflicting cross-border compliance burdens, and ensure a genuinely unified defense against transnational cyber threats.
#3 **CRA reporting obligations**	
Provisions concerned: Article 14(1) Cyber Resilience Act (Regulation (EU) 2024/2847)	
Current situation: Article 14, provision 1 requires reporting actively exploited vulnerabilities to the coordinating CSIRT.	
Practical Challenge & Business Impact	**Proposed recommendation**
This requirement poses a variety of security and legal risks for companies, including: • Undermining the best practice that the fewer who know about an unpatched vulnerability, the better; • The coordinating CSIRT may be targeted by the threat actor, and may itself have inadequate safeguards in place;	Add language to the end of 14(1) that says, “manufacturers can delay the compliance with this requirement due to conflicting contractual requirements or countervailing security concerns.” Add language in 14(1) mandating reporting vulnerabilities only after mitigations are available.

• When companies share information about exploited vulnerabilities with other companies, they are typically required to keep such information confidential.	
#4 **CRA: definitions and operational details of essential cybersecurity requirements**	
Provisions concerned: Articles 3 and 24 and Annex I Cyber Resilience Act (Regulation (EU) 2024/2847).	
Current situation: The CRA establishes a horizontal framework of essential cybersecurity requirements for products with digital elements, which entered into force on December 10, 2024. However, the foundational text of the Regulation leaves the precise definitions and operational details of several critical concepts to "to-be-determined" future guidance, delegated acts, and implementing acts. For example, the Commission is mandated to issue future guidance to clarify what constitutes a "substantial modification". Similarly, the distinction between an in-scope Remote Data Processing Solution (RDPS) and an out-of-scope outsourced cloud service (SaaS/PaaS) is currently relegated to draft guidance that is still posing fundamental questions about how to define "at a distance" and assess system boundaries. Despite these open questions, the strict enforcement deadlines,September 2026 for reporting and December 2027 for full compliance, remain fixed.	
Practical Challenge & Business Impact	**Proposed recommendation**
Enacting binding legal obligations while leaving the technical and operational details to future guidance creates severe compliance gridlock and operational risks for manufacturers: When critical details—such as the exact technical specifications for product categories or the harmonised standards required to demonstrate conformity—are delivered late, manufacturers are forced to design products based on anticipated, rather than finalized, requirements. Without finalized guidance on scoping (such as whether a specific cloud integration qualifies as an RDPS requiring full CRA compliance or a third-party SaaS requiring only due diligence), companies cannot accurately plan their compliance roadmaps. Furthermore, if harmonised standards are delayed, manufacturers will be forced into costly and time-consuming third-party conformity assessments, risking significant delays in getting products to market. A "substantial modification" shifts the entire burden of manufacturer obligations to the entity making the modification. Without clear, finalized guidance defining this threshold, third-party developers, importers, and even original manufacturers operate under a cloud of legal	The enforcement dates of the CRA, and any similar legislation, should be strictly contingent upon the timely delivery of all necessary supporting documentation. Harmonized standards and critical guidance (such as those defining RDPS and substantial modifications) must be finalized and published at least 12 to 18 months prior to the enforcement date. If this guidance is delayed, the enforcement timeline must be correspondingly extended to give industry sufficient time to implement the rules. While detailed EU-specific guidance and harmonised standards are pending, the Commission should explicitly recognize widely adopted international security frameworks and existing industry certifications as a valid means of demonstrating compliance. Establish a clear safe harbor or grandfathering pathway for products that enter their development cycles while critical guidance remains in a draft or TBD state, ensuring companies are not retroactively penalized for good-faith design choices.

uncertainty, risking severe penalties (up to €15 million or 2.5% of global turnover) for unintentional non-compliance.	
#5 **CRA "early warning" notification**	
Provisions concerned: Article 14(2)(a), Article 14(2)(b) and Article 14(4)(a) of the CRA	
Current situation: The Cyber Resilience Act (CRA) requires manufacturers to submit an "early warning" notification for actively exploited vulnerabilities and severe incidents within a strict 24-hour window of becoming aware of the event, followed by a more detailed notification within 72 hours. This adds to a highly complex and fragmented landscape of EU regulatory regimes—such as NIS2, DORA, and the AI Act—that mandate incident reporting under different criteria and to different authorities. Notably, the GDPR already establishes a standard that a data breach must be reported to the relevant supervisory authority within 72 hours of discovery if it is likely to imperil individuals' rights and freedoms.	
Practical Challenge & Business Impact	**Proposed recommendation**
These duplicative, dissonant, and aggressive reporting requirements create an enormous administrative burden. A 24-hour reporting deadline forces organizations to divert highly specialized, scarce incident response personnel away from crucial active threat investigation, containment, and mitigation efforts. Instead of focusing on resolving the active incident and protecting users, security teams must scramble to fill out differing templates for various regulators across potentially 27 EU Member States. This premature reporting mandate ultimately hinders, rather than helps, the overarching goal of rapid and effective incident response.	Amend CRA articles 14(2) (a & b) and delete 14(4)(a) to revise and standardize incident reporting timelines across the CRA and other frameworks around a 72-hour deadline. Aligning with the existing GDPR 72-hour standard promotes consistency and reduces the overlapping compliance burdens placed on scarce incident response personnel.
#6 **CRA: awareness threshold**	
Provisions concerned: Article 14 CRA	
Current situation: Under Article 14 of the Cyber Resilience Act (CRA), manufacturers are legally obligated to submit an early warning notification to the designated CSIRT and ENISA within a strict 24-hour window of "becoming aware" of an actively exploited vulnerability or a severe incident. However, the foundational text lacks a precise, harmonized definition of exactly when this "awareness" threshold is officially crossed. This ambiguity creates friction with other existing European regulatory regimes, such as the GDPR and the NIS2 Directive, which have their own reporting triggers and operational interpretations.	
Practical Challenge & Business Impact	**Proposed recommendation**
In large-scale digital enterprise environments, automated security systems generate thousands of raw signals and alerts daily, many of which turn out to be false positives or benign anomalies. If the 24-hour regulatory clock is interpreted to start the moment a raw alert is generated—before human	Regulatory guidance should explicitly harmonise the definition of "becoming aware" across the CRA, NIS2, and GDPR (we welcome and would encourage following the EDPB guidance on this in the GDPR).

experts can investigate—organizations will be forced to defensively over-report unverified events to avoid severe non-compliance penalties. This flood of premature reports will clog the ENISA single reporting platform with "noise," degrading the situational awareness of national CSIRTs. Furthermore, it diverts scarce and highly specialized incident response personnel away from actively investigating and mitigating the threat, forcing them instead to draft legal notifications before the nature or severity of the incident is even understood.	The timeline for reporting should only commence after a suspected event has been initially triaged and verified by the manufacturer's appropriate incident response team. Aligning the start of the clock with the moment an organization has reasonably confirmed that an event actually meets the legal thresholds of a "severe incident" or "actively exploited vulnerability" prevents false alarms, aligns with established GDPR practices, and ensures that regulators receive highly actionable, accurate threat intelligence.
#7 **CSA 2.0: security impact assessments**	
Provisions concerned: Articles 4(3), 5(1)(h), 5(5) and 8(4) draft Cybersecurity Act (CSA) revision.	
Current situation: Lack of a "secure-by-design" approach and Security Impact Assessments (SIA) in policymaking. The current mandate implies ENISA only assists with cybersecurity laws like the CRA or NIS2, and its involvement depends on requests from the EDPB or the Commission. It does not explicitly empower ENISA to assess "non-security" laws (such as the Digital Markets Act or Data Act) that might inadvertently undermine security.	
Practical Challenge & Business Impact	**Proposed recommendation**
Non-security regulations can accidentally weaken digital defenses, such as transparency requirements that adversaries could exploit to poison production models. Furthermore, addressing security risks late in the legislative cycle or during implementation is significantly more expensive than addressing them during the design phase.	Empower ENISA to conduct Security Impact Assessments to evaluate policies from a cybersecurity perspective as part of the official impact assessment and implementation processes. We recommend updating Articles 4(3), 5(1)(h), and 5(5), and adding a new Article 8(4) of the current draft CSA revision text, to formally integrate the SIA into the legislative process and ensure continuous proactive oversight.

Cloud

This section sets out targeted simplification proposals across the review of the **Public Procurement Directives**, and the proposed **Digital Networks Act (DNA)**. The recommendations focus on: (i) avoiding new, overlapping obligations in an already crowded regulatory space and ensuring coherence with existing EU legislation; (ii) modernising public procurement so it better reflects the dynamics of **Software as a Service (SaaS)**, continuous security and AI updates, and technology-neutral, outcome-based purchasing; and (iii) strengthening legal certainty under the DNA by refining key definitions and scope in binding legislative text, rather than relying on explanatory materials

<table>
<tr><td colspan="2">#1 Public Procurement Directives Review and DG CONNECT Recommendation for cloud procurement in the public sector</td></tr>
<tr><td colspan="2">Provisions concerned:
Public Procurement Directives</td></tr>
<tr><td colspan="2">Current situation:
We believe that the current framework must be updated to bridge the gap between rigid administrative law and the fast-paced nature of technological progress needed to achieve citizens' proximity, efficiency and create the baseline for economic competitiveness and interoperability. To unlock the potential of the Single Market and Artificial Intelligence (AI), we call for a framework grounded in market-based competition, transparency through digitization, technology neutrality, and the cross-border free movement of services.</td></tr>
<tr><td>Practical Challenge & Business Impact</td><td>Proposed recommendation</td></tr>
<tr><td>The revision of the Directives offers a unique opportunity to transform procurement from a pricing tool into a strategic investment mechanism. A procurement geared towards long-term contractual relationships and moving away from set-and-forget models can provide better access to best-in-class innovation solutions.</td><td>Simplification of the public procurement rules: It will not only support innovation and SME participation but will specifically help to address the disconnect between static procurement rules and the dynamic Software as a Service (SaaS) market. This is necessary because existing rules generally reflect a perspective of physical goods and services that have a final stage of finishing.

Strategic Shift & Market-Based Competition: Evolve procurement into a strategic, outcome-focused tool based on transparency, efficiency, technology neutrality, and cross-border free movement.

Value & Technology Neutrality: Prioritize the Best Price-Quality Ratio (BPQR) and a lifecycle view over lowest-price bidding. Focus on functional, performance-based requirements rather than proprietary features or specific brands.

Standardization & Consistent Risk Assessment: Conduct standardized Data Processing Impact Assessments to avoid duplication. Default to open-source technology and compliance with widely accepted international security standards. Create clear definitions and consistent obligations across legislation to guarantee legal certainty.

Cloud-Specific Rules & Service Evaluation: Introduce special rules reflecting the dynamic nature of Software as a Service (SaaS), such as pay-as-you-go models and continuous security developments. These rules must allow for the evaluation of the service itself instead of fixed</td></tr>
</table>

	requirements at a specific point in time, and permit changes to terms and services to accommodate continuing developments with AI. Agile Procedures & Dynamic Purchasing: Expand the broader use of (the fully electronic) Dynamic Purchasing Systems (DPS) and digital marketplaces to streamline the admission phase, ensuring the public sector has continuous access to new SaaS players and the latest innovations. Standardized "Cloud-Ready" Contracts, Data & Clauses: Promote EU-wide standardized templates for Service Level Agreements (SLAs), data portability, and exit strategies to reduce the burden on public buyers, preventing the need for them to hire specialized legal counsel to draft complex terms. The portability of underlying data must become a priority for IT teams supporting cloud procurements. Simplified Competitive Procedures with Negotiation: Make it easier to justify negotiated procedures so buyers can discuss complex integration and security requirements prior to final bids, significantly reducing the risk of a "failed" tender due to impossible or overly restrictive requirements. Modernized Innovation & Light-Weight PoCs: Expand the modern definition of innovation to explicitly include process digitization and the application of AI. Recommend streamlined mechanisms for light-weight Proof of Concepts (PoCs) to test technologies with limited implementation burdens before scaling. Innovation Partnerships & Societal Challenges: Use flexible instruments and Innovation Partnerships to combine existing market-ready cloud services and AI tools in novel ways to address public sector needs. This focus on functional, performance-based requirements—rather than component novelty—will facilitate the creation of complex, multi-vendor ecosystems without unnecessary administrative barriers.

	Utilize updated procedures for completely new methods solving societal challenges, such as streamlining citizen services or optimizing energy grids with AI. Ensure legal conditions for utilizing Innovation Partnerships and similar flexible instruments like the Competitive Dialogue are clear so authorities have the confidence to employ these flexible vehicles. Process Efficiency & Transparency: Digitize procurement with a single-entry marketplace, establish a unified Foreign Subsidies Regulation (FSR) declaration portal, and require buyers to publish intent to award at least one year in advance. Keep specific sectoral requirements (defense, intelligence) separate from the general framework. Flexible Contracts & Concession Durations: Allow for dynamic contract clauses accommodating technological evolution, and extend concession or contract durations to 10-15 years to justify technical innovation and environmental investments. Clarify definitions of concessions and operating risk for global risk-assessment models. Sustainability & Permitting: Incentivize Green Public Procurement by rewarding providers who use locally and hourly matched carbon-free energy. Streamline and digitize pre-permit review mechanisms to accelerate the establishment of vital data centers. Digital Skills & AI Enablement: Invest in specialized education and digital skills training for the public sector to effectively procure and manage cloud and AI technology. Align procurement strategies with key pillars for maximizing AI value, such as citizen-centric service delivery and operational efficiency.
#2 **Digital Networks Act**	
Provisions concerned: Article 2; Article 191 - 193	
Current situation:	

The current EECC, as transposed by most Member States, primarily regulates providers of public ECNs and publicly available ECSs. However, the proposed Digital Networks Act (DNA) expands this scope to include non-public ECNs used mainly for public information society services and related sectors.

- Definition of electronic communications network (ECN) (Art. 2(1)): The definition continues to be worded without reference to provision of ECS and has a broad scope: Every transmission system used to transmit signals is covered, and ECN include content delivery networks (CDN), cloud networks, backbone networks, etc.
- Definition of interconnection (Article 2(29) and Recital 15): The DNA seeks to remove any limitation of interconnection to public networks. Therefore, interconnection now covers both public and private ECN.
- General Authorisation (Article 2(23)): The DNA mandates application of the general authorization regime not only for public ECN, but also for non-public ECN that are wholly or mainly used for the provision of information society services to the public. Providers of such non-public ECN are also subject to the resilience obligations introduced by the DNA.
- Ecosystem cooperation (Art. 191 to 193): The rules on ecosystem cooperation (which have no equivalent in the EECC) are drafted with an even broader scope: They are to apply to all providers of public and non-public ECN and to other undertakings active in the electronic communications or closely related sectors. Examples for such closely related sectors provided by the DNA include cloud providers and content and application providers (cf. Rec. 404)

Practical Challenge & Business Impact	**Proposed recommendation**
The proposal's unclear scope could expand the definition of regulated entities beyond traditional telecom operators to potentially include cloud providers and Content Delivery Networks (CDNs). This would be a regulatory overreach. The extension of the interconnection definition to non-public ECS is relevant in particular in relation to the risk that National Regulatory Authorities could seek to impose interconnect and access requirements, and in relation to the voluntary conciliation procedure. The DNA will bring various non-public ECN and network elements in scope of mandated regulation, including international interconnections, aggregation networks, core and backbone networks, submarine communication cables (including their cable landing stations), satellite networks integrated with terrestrial networks which are capable of providing back-up service in the event of unavailability of any of these networks, content delivery networks or networks connecting large data centre facilities. In relation to non-public ECN, it is key for the application of the general authorization regime/the	Strengthen the legal certainty by refining the definitions in Article 2. Relying on the Explanatory Memorandum is insufficient, as it lacks the binding force necessary to protect non-telecom entities from misclassification

resilience obligations, whether such networks are used mainly for the provision of information society services to the public. Given the broad scope of the term 'information society service', this will cover any ECN that is at least mainly used for the provision of cloud services, online platforms, search engines, streaming services, online market places, online media, online banking and insurance service, among others. The DNA does not define the scope of "closely related sectors" in the context of ecosystem cooperation. Based on the Recitals, this is to include cloud providers and content and application providers. While the DNA states that it does not seek to regulate cloud service providers directly, there is a risk that the ecosystem cooperation, and in particular the voluntary conciliation procedure, will lead to regulatory scrutiny of previously purely commercial agreements.	

Digital Identity

The recommendations address: (i) the need for **technical stability**; (ii) **regulatory synergy and predictability** across eIDAS 2.0, the GDPR, and the DSA/DMA,; and (iii) **broad accessibility through technological neutrality**, ensuring that certification requirements remain outcome-focused so that a wide range of secure solutions can meet the standard and the Wallet can be adopted at scale.

#1 **Facilitating a seamless transition through technical stability**	
Provisions concerned: Article 5a (European Digital Identity Wallets) & Implementing Acts	
Current situation: The eIDAS 2.0 framework is a pioneering effort requiring approximately 40 - 50 implementing acts to define the detailed technical specifications of the Wallet and the underlying digital identity infrastructure. As Member States and relying parties begin their development cycles, they are navigating an evolving landscape where the architecture reference framework (ARF) and legal clarifications in the form of implementing acts are being finalized in parallel.	
Practical Challenge & Business Impact	**Proposed recommendation**
For global platforms and relying parties eager to support the Wallet, the primary challenge is ensuring that early engineering investments align with the final, certified standards.	We suggest that the 24-month implementation period for relying parties be benchmarked against the final publication of the core implementing acts. This "technical readiness" approach ensures that the ecosystem is built on a stable foundation,

• Operational Optimization: Clear and finalized technical specifications are the most critical driver for adoption. When technical protocols are refined during the implementation phase, it requires significant iterative engineering. Providing a stable technical baseline early in the process will help all stakeholders allocate resources more efficiently and accelerate the rollout. • Implementation Readiness: Large-scale infrastructure changes in regulated sectors typically require significant lead times. Aligning the compliance window with the availability of final, stable technical standards ensures that "fitness" is built into the system from day one.	minimizing the need for retroactive adjustments and maximizing system reliability.

#2 **Fostering regulatory synergy**	
Provisions concerned: Interaction between eIDAS 2.0, GDPR, and the DSA/DMA.	
Current situation: The EUDI Wallet will be a cornerstone of the EU's broader digital strategy, intersecting with data protection (GDPR) and platform regulation (DSA/DMA). Success depends on a unified interpretation of requirements across these different regulatory domains.	
Practical Challenge & Business Impact	**Proposed recommendation**
Governance Synergy: Implementation is most effective when technical (security) standards and data protection principles are interpreted through a single, cohesive lens. For instance, it should be ensured that "selective disclosure" mechanisms comply with all of the following regulatory requirements: the eIDAS technical certification; the GDPR data minimization principle; and the Article 28(3) DSA requirement that providers of online platforms should not process additional personal data in order to assess whether a user is a minor. Additionally, EUDI Wallets should be considered to be a valid means of age verification by regulators and DSA auditors, in line with the Commission's Article 28 DSA Guidelines. Regulatory Predictability: Private parties often face overlapping obligations, such as "Strong User Authentication" (SCA) requirements in different regulations. A cohesive approach to how the EUDI	We recommend formalizing a structured dialogue between the eIDAS Cooperation Network and other relevant authorities, such as the European Data Protection Board (EDPB) and the European Board of Digital Services (EBDS). This collaborative approach could produce joint implementation guidelines that offer "one-stop-shop" clarity for relying parties, ensuring that a certified EUDI Wallet will be recognized as also fulfilling relevant privacy requirements across the digital regulatory landscape.

Wallet will fulfill these multiple roles will provide the legal certainty needed to drive widespread investment in the ecosystem.	
#3 **Ensuring broad accessibility and technological neutrality**	
Provisions concerned: Article 5a(11) – Certification of Wallets.	
Current situation: The "High" Level of Assurance (LoA high) required for the EUDI Wallet is a vital component of its security architecture. Achieving this level of trust requires a sophisticated blend of hardware-backed security and innovative software solutions.	
Practical Challenge & Business Impact	**Proposed recommendation**
Inclusive Innovation: To ensure the EUDI Wallet is accessible to every European, regardless of their device, it is important to maintain a technology-neutral approach to "LoA High." This encourages a diverse range of secure solutions, including both hardware-based and advanced software-based security models. Universal Reach: A flexible, performance-based certification framework helps prevent a "digital divide," ensuring that the Wallet works seamlessly across a wide spectrum of mobile devices while maintaining the highest security standards.	We recommend that the upcoming implementing acts on certification focus on security outcomes rather than specific hardware dependencies. By encouraging a variety of technical paths to achieve "LoA High", the Commission can ensure the EUDI Wallet is inclusive, innovative, and ready for universal adoption across the Union.

Conclusion

The European Union has set itself a worthy ambition: to shape a digital economy that is secure, trusted, resilient and fair. Yet ambition alone will not suffice. If this project is to succeed, the regulatory framework underpinning it must also be coherent, proportionate and capable of working in practice. Where several instruments govern the same issue in parallel, it is a necessary means of ensuring that the rules are clearer, more consistent and ultimately more effective. The recommendations set out above are intended to reduce duplication, clarify the relationship between overlapping instruments, and foster a more stable and predictable environment for businesses operating across the Single Market. In doing so, they would enable companies to devote a greater share of their resources to innovation, security, consumer protection and competitiveness, instead of dispersing their efforts across fragmented and repetitive compliance requirements. BSP therefore calls to streamline the existing body of digital rules, update provisions that no longer reflect technological and commercial realities, and reinforce harmonisation across the Union.

Rue Belliard 40, 1000 Brussels
e-mail: info@zpbsp.com
EU Transparency Register Number: 548212735276-89

About BSP

Business & Science Poland (BSP) combines the experience of leading Polish enterprises with the EU agenda. We represent the knowledge and interests of Polish companies employing over 180,000 people in Poland, the EU, and globally. Our goal is to support the EU Single Market in line with the need for its responsible and effective transformation. This opinion presents the position of BSP members representing the digital, financial, air transport, fertiliser, chemical, mining, refining, fuel and energy sectors.

Rue Belliard 40, 1000 Brussels
e-mail: info@zpbsp.com
EU Transparency Register Number: 548212735276-89