Position Paper on the Proposal for a Digital Omnibus Regulation

# Grounding simplified EU digital rules in operational reality and legal certainty

**February 2026**

The Computer & Communications Industry Association (CCIA Europe) welcomes the European Commission's Digital Omnibus proposal as a necessary step to reduce the regulatory complexity and fragmentation hindering Europe's competitiveness. While the proposal takes important steps towards simplification, it also risks introducing new complexities, for example in browser-based consent. CCIA Europe offers the following recommendations to ensure the Omnibus delivers a simpler, faster, and more robust rulebook – one anchored in legal certainty and benefitting technology and digital companies of all sizes operating across the EU.

## I. Strengthening GDPR for the AI era

*The Omnibus aims to modernise the General Data Protection Regulation (GDPR) by clarifying personal-data definitions and recognising legitimate interest as a legal basis for AI training. However, in order to truly deliver, lawmakers must provide additional legal certainty.*

### Recommendations:

1. Ensure 'legitimate interest' for AI training is practical and harmonised
2. Clarify definition of personal data, based on clear and proportionate criteria
3. Refocus special categories of data definitions and broaden derogations
4. Introduce essential clarifications on automated decision-making

## II. Restoring coherence across privacy and data laws

*Overlapping rules and conflicting definitions continue to frustrate businesses and users alike. The Digital Omnibus must resolve conflicts between the Data Act and GDPR, unify terminal equipment processing rules, and reduce consent fatigue.*

### Recommendations:

5. Consolidate and unify rules for terminal equipment-related processing
6. Oppose mandatory browser consent, 'six-month no re-ask,' and media exemption
7. Resolve the conflict between data-portability rights and gatekeeper restrictions
8. Harmonise DPIAs and enforce 'One Assessment' principle across laws

## III. Harmonising cybersecurity compliance

*The proposed single-entry point for incident reporting is a good first step. Yet, technical tools alone cannot solve fragmentation if timelines, thresholds, and templates still differ across the GDPR, NIS2 Directive, Cyber Resilience Act, and the Digital Operational Resilience Act.*

### Recommendations:

9. Ensure 'single-entry point' integration and industry consultation
10. Establish a unified incident-reporting standard across laws

# Introduction

The Computer & Communications Industry Association (CCIA Europe) welcomes the European Commission's proposal for a Digital Omnibus Regulation. This much-needed initiative comes at a crucial point in time, recognising that the accumulation of EU digital rules over the past legislative term has created unprecedented complexity, fragmentation, and administrative burdens that undermine Europe's competitiveness.

The Omnibus proposal takes important first steps toward simplifying and consolidating existing digital rules, for instance by unifying data requirements and creating a single-entry point for reporting cybersecurity incidents.

Yet, in its current form, the proposed Regulation risks introducing new complexity in critical areas such as browser-based consent. More can also be done to better ground digital rules in operational realities and to anchor the much-need improvements in legal certainty, delivering meaningful simplification while strengthening safeguards.

CCIA Europe offers the following recommendations to ensure the proposal fulfills its promise of a simpler, faster, and more robust digital rulebook that benefits technology and digital companies of all sizes operating across the EU:

I. Strengthening GDPR for the AI era
II. Restoring coherence across privacy and data laws
III. Harmonising cybersecurity compliance

# I. Strengthening GDPR for the AI era

*The Omnibus aims to modernise the General Data Protection Regulation (GDPR) by clarifying personal-data definitions and recognising legitimate interest as a legal basis for AI training. However, in order to truly deliver, lawmakers must provide additional legal certainty.*

## 1. Ensure 'legitimate interest' for AI training is practical and harmonised

CCIA Europe welcomes the introduction of Article 88c of the Omnibus, which codifies that the training of AI models can constitute a legitimate interest in line with Opinion 28/2024 of the European Data Protection Board (EDPB).[1] However, by introducing specific, undefined conditions for AI that diverge from Article 6(1)(f) of the General Data Protection Regulation (GDPR) in its current form, the proposal risks invalidating decades of jurisprudence and guidance.

Specifically, limiting the use of legitimate interest(s) as a legal basis for processing personal data to the controller alone diverges from 'third-party' interests, which EU data protection laws have always allowed for the past three decades.[2] In practice, this limitation means that downstream SMEs that fine-tune or deploy AI models for specific applications (e.g.

[1] Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, 17 December 2024, https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en
[2] See Art. 6(1)(f) GDPR, and Art. 7(f) Data Protection Directive 95/46/EC;

healthcare startup using a pre-trained model) may be unable to legally use pre-trained models because they are unable to demonstrate that the model's original training served their specific legitimate interests, even though the GDPR has consistently allowed relying on the model developer's legitimate interests as a third party.

In addition, the provision allowing 'national laws' to explicitly require consent and to override this article is a capitulation to regulatory fragmentation. It invites the creation of 27 divergent national regimes for AI training, directly contradicting the CJEU's ASNEF ruling against national measures that preempt the legitimate interest balancing test.[3]

Finally, CCIA Europe strongly cautions EU lawmakers against adopting language that would codify technically erroneous concepts in relation to AI models, specifically references to 'residually retained data', 'data memorised' and 'storage.'[4] These terms wrongfully suggest that AI models function as databases that memorise personal data, rather than systems learning abstract patterns. This is false. Generative AI models do not store copies of their training data. Instead, they learn patterns and concepts as numerical weights, similar to someone who reads several books on a subject and then writes their own. Generative AI doesn't copy but analyses information, enabling it to create original content.[5] Legislating based on this disputed premise risks prejudging complex intellectual property questions currently debated in separate policy and legal forums.

**Call to action:** CCIA Europe urges EU lawmakers to avoid creating two separate legal bases for 'legitimate interest' under the General Data Protection Regulation (GDPR), and instead suggests to fully align Article 88c with Article 6(1)(f) GDPR by explicitly including 'third-party' interests and deleting the provision that allows national laws to mandate consent. Additionally, references to technically inaccurate concepts such as 'retained,' 'memorised,' or 'stored' data should be removed to ensure the Regulation addresses AI technologies accurately, without mischaracterising their functioning or inadvertently inviting copyright-related debates in other forums.

## 2. Clarify definition of personal data, based on clear and proportionate criteria

The proposed amendment to Article 4(1), clarifying that data is not 'personal' for a specific entity if that entity cannot reasonably identify an individual, codifies the CJEU's Breyer and SRB decisions.[6] This is a welcome, essential step to correct diverging regulatory interpretations that have treated data as personal, even when identification by the controller was practically impossible without illicitly accessing third-party data. However,

[3] Joint cases ASNEF and FECEMD (C-468/10 and C-469/10), https://infocuria.curia.europa.eu/tabs/document?source=document&docid=115205&doclang=EN&mode=&part=1;
[4] Wording used in Recital 33, Article 9(5), Article 88c of Digital Omnibus proposal
[5] For further discussion, see CCIA Europe, Generative AI & Copyright in the EU: Myths Versus Facts (June 2025), https://ccianet.org/articles/generative-ai-copyright-in-the-eu-myths-versus-facts/#Copies_Training_. See also Getty Images (Trading) Ltd v Stability AI Ltd [2025] EWHC 3090 (Ch) (Nov. 2025), where the UK High Court accepted technical evidence that AI models do not store copies of training data (at paras. 430, 552-559), https://www.judiciary.uk/wp-content/uploads/2025/11/Getty-Images-v-Stability-AI.pdf;
[6] See Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland establishing that data (like dynamic IP addresses) is personal data if the controller has the legal means to identify the individual (e.g. by compelling an ISP to provide the name) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0582, and Case C-413/23 European Data Protection Supervisor v Single Resolution Board ruling that data might be 'personal' for the sender (who holds the decryption key) but not 'personal' for the recipient (who lacks the reasonable means to re-identify the subjects), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62023CJ0413

relying solely on the concept of 'reasonable means' without specifying what it means, risks perpetuating the current fragmentation, where some supervisory authorities apply theoretical rather than practical standards of identifiability.

To ensure consistent enforcement and prevent regulatory overreach, the final legal text must explicitly codify the objective criteria for the 'reasonable means' test. Furthermore, the Commission's empowerment to specify criteria for pseudonymisation (new Article 41a) should be used to provide practical guidance on how technical safeguards, such as state-of-the-art pseudonymisation techniques, factor into the assessment of whether data remains personal for a specific controller.

**Call to action:** Co-legislators should support the proposed codification of EU case law, shifting to a practical, implementable definition of personal data. However, amendments are needed in Article 4(1) GDPR to explicitly list objective factors for what 'reasonable means' refers to, including costs, time, technological resources, and legal safeguards to the entity, in order to guarantee unambiguous criteria for reasonable means of identification in practice. Co-legislators should also clarify in Recital 26 GDPR that technical identifiers processed solely for security and performance purposes by intermediaries lack the 'means reasonably likely' for identification. For controllers who do not hold a direct billing or account relationship with an end-user (e.g. content delivery networks and DDoS mitigation services), technical signals like IP addresses should be explicitly recognised as non-personal data in their hands. Additionally, CCIA Europe supports the introduction of Article 41a to provide technical certainty on when safeguards such as pseudonymisation effectively render data non-personal.

## 3. Refocus special categories of data definitions and broaden derogations

The Omnibus aims to permit ;legitimate interests; as a legal basis for AI model training, but fails to address the growing problem of how regulators define Special Categories of Data under Article 9(1) GDPR. Indeed, enforcement trends increasingly classify ordinary data as 'sensitive' based on theoretical inferences, regardless of whether the controller actually intends to infer sensitive attributes. Without managing to successfully fix this foundational issue and refocusing the definition on real-world processing purposes rather than speculative potential, the new AI derogation will remain largely unusable.

In addition, the conditions in the proposed Article 9(5) GDPR are unworkable in their current form. Requiring AI developers to 'avoid' collecting sensitive data from large-scale datasets is both technically impossible and counterproductive. In practice, it would force them to proactively identify and label sensitive information they would otherwise ignore. A more practical approach would be to impose risk-mitigation and technical safeguards to ensure appropriate management of identified special categories of data.

Finally, to ensure technology-neutral protections that support essential services beyond AI, the derogations in Article 9(2) should be expanded to include processing based on legitimate interest and contractual necessity, once again subject to appropriate safeguards.

**Call to action:** Lawmakers should amend Article 9(1) GDPR to limit the definition of Special Categories of Data to information that is actually used to infer or directly reveal sensitive attributes. In addition, Article 9(5) GDPR should replace the obligation to 'avoid' collection with a requirement to 'mitigate risk' via technical measures, and remove mandatory output

filters that degrade system performance. Finally, Article 9(2) should include new derogations for processing based on legitimate interest and contractual necessity, ensuring the framework remains technology-neutral.

### 4. Introduce essential clarifications on automated decision-making

CCIA Europe welcomes the Commission's proposal to amend Article 22(2)(a) of the GDPR, clarifying that automated decision-making is permissible for contract performance, even when a human could theoretically perform the same task. This technical correction helps modernise the 'necessity' test and prevents courts from treating automation as a last resort, rather than a valid tool for efficiency. However, this amendment alone doesn't solve the underlying problem: Article 22 lacks a clear definition of 'legal or similarly significant effects' which is the threshold that triggers user rights and processing restrictions.

Without a clear definition, some supervisory authorities will continue to interpret Article 22 so broadly that nearly any algorithmic processing or personalisation could qualify as 'high-risk' automated decision-making. This expansive reading deviates from the legislature's intent and creates unnecessary compliance burdens for low-risk AI applications. To focus Article 22 on genuine risks, the Omnibus should codify the threshold established by the CJEU in SCHUFA.[7] Specifically, 'similarly significant effects' should be limited to factors that decisively determine a person's legal status, rights, or entitlements, or have a comparable prolonged and structural impact (e.g. processing that results in systemic financial exclusion), rather than transient or minor algorithmic interactions.

**Call to action:** Lawmakers should retain the amendment to Article 22(2)(a) ensuring automation is valid for contract performance regardless of whether a human could perform the task. Lawmakers should also consider adding a new paragraph defining 'legal or similarly significant effects' to clarify that Article 22 applies only to decisions that decisively determine a data subject's legal status or have prolonged, structural impact on an individual.

## II. Restoring coherence across privacy and data laws

*Overlapping rules and conflicting definitions continue to frustrate businesses and users alike. The Digital Omnibus must resolve conflicts between the Data Act and GDPR, unify terminal equipment processing rules, and reduce consent fatigue.*

### 5. Consolidate and unify rules for terminal equipment-related processing

Moving Article 5(3) of the ePrivacy Directive into the GDPR – per Article 88a of the Omnibus proposal – is the right ambition to centralise enforcement, but the current draft creates a legally hazardous split regime that defeats the purpose of simplification. By limiting the transfer to the processing of personal data, while leaving non-personal data under the legacy ePrivacy Directive, the proposal ignores the technical realities of the internet: a single file, cookie, or beacon often processes both types of data simultaneously or sequentially.

[7] Judgement of the Court of 7 December 2023, Case C-634/21, available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0634

Consequently, businesses would face a scenario where the exact same technology is subject to supervision by data protection authorities under the GDPR and simultaneously by 27 national telecom regulators under national e-Privacy implementations. To achieve genuine simplification and legal certainty, co-legislators should repeal Article 5(3) of the ePrivacy Directive in its entirety and consolidate all terminal equipment rules into the GDPR, ensuring a single, consistent enforcement mechanism.

The exemptions proposed in Article 88a(3) are far too narrow to meaningfully reduce consent fatigue or incentivise privacy-centric business models. The exemption for audience measurement is currently restricted to 'aggregated' processing carried out "solely for its own use" by the controller. In practice, this limitation disproportionately penalises smaller players, such as SMEs and independent publishers, who rely on third-party vendors for measurement.

Regrettably, the proposal fails to meaningfully reduce reliance on consent by keeping a broad range of everyday, low-risk uses within a blanket opt-in model. The volume of consent banners will not decrease if low-risk activities continue to remain non-exempt, with the ecosystem remaining locked into a consent-heavy framework that frustrates users and harms the ad-supported web. In particular, the proposal should exempt first-party cookies used for analytics – including processing of personal data where necessary to support the provision, security, and improvement of an online service requested by the user – provided that the use is strictly limited to analytics. The proposal should also exempt functional cookies used for user-requested personalisation of the online service (e.g. remembering user-selected language, region, accessibility and display settings, items in a basket, saved sizes, or preferred merchants). The proposal should also exempt minimal, low-risk processing for the purpose of contextual advertising (including strictly necessary technical delivery functions like frequency capping and fraud prevention).

**Call to action:** Co-legislators should fully repeal Article 5(3) of the ePrivacy Directive and transfer all terminal equipment rules to the GDPR to prevent a dual enforcement regime. In addition, Article 88a(3) must be expanded to exempt first-party analytics for the provision, security, and improvement of online services requested by users, third-party functional cookies, third-party audience measurement, and contextual advertising from consent requirements.

## 6. Oppose mandatory browser consent, 'six-month no re-ask,' and media exemption

The introduction of Article 88b, mandating automated machine-readable indications of user choice, is fundamentally flawed and contradicts the Omnibus's primary objective of simplification. Far from streamlining the EU digital acquis, this provision effectively creates a parallel regime for consent management that duplicates existing GDPR mechanisms, thereby introducing profound legal and technical uncertainty. Previous attempts to impose such signals, such as the 'Cookie Pledge' or various iterations of the ePrivacy Regulation proposal, have consistently failed due to insurmountable technical complexity and a lack of consensus.

Crucially, a centralised, binary signal coming from the user's internet browser cannot meet the GDPR's high threshold for 'specific' and 'informed' consent without rendering the user interface completely unusable. The proposal for a broad signal, renewed every six months,

fails to provide the granular detail required to validly consent to specific processing purposes across millions of unique websites. Website owners, who must retain the ability to engage directly with their customers, will thus remain legally entitled to display banners to request specific permissions or overrides.

As a result, Article 88b will not reduce consent fatigue but rather create more confusion – compelling users to navigate conflicting consent signals between their browser settings and website interfaces. By mandating specific technical implementations, the proposal also undermines the principle of technological neutrality, erecting browsers as the de facto gatekeepers of the internet.

Furthermore, the proposed exemption for media service providers in Article 88b(3) creates an unjustified two-tier internet that arbitrarily picks market winners and losers. This is discriminatory by nature. And while intended to protect independent journalism, this carve-out fails to recognise that the digital ecosystem is deeply interconnected. Media publishers rely on third-party advertisers and cross-site data from non-exempt sectors to validate ad inventory and monetise content.

If the broader ecosystem is blocked by mandatory signals, the media sector inevitably loses the data flows necessary to sustain its revenue, rendering the exemption economically ineffective in addition to being legally discriminatory. By allowing one category of controllers to ignore user signals while binding others, the proposal destroys regulatory coherence and fundamentally undermines user trust in the protection of their data.

**Call to action:** Co-legislators should delete Article 88b altogether to avoid establishing a technically unworkable and discriminatory consent framework that would further fragment Europe's Single Market.

## 7. Resolve the conflict between data-portability rights and gatekeeper restrictions

The Omnibus proposal misses a critical opportunity to resolve a fundamental contradiction within the EU rulebook that currently traps businesses in a compliance deadlock. Indeed, Article 5(2) of the Data Act prohibits gatekeepers from acting as authorised third parties for data access – a restriction that stands in direct opposition to the user's portability rights guaranteed under Article 20 GDPR and the contestability measures of Article 6(9) of the Digital Markets Act (DMA).

This regulatory friction forces all companies holding user data into an untenable position: fulfilling a valid user request to port data to a gatekeeper violates the Data Act, while refusing that same request invites liability under the GDPR and DMA.[8] The Commission recently suggested that Article 5(2) applies only to 'mandatory' data-sharing mechanisms and leaves 'voluntary arrangements' unaffected, reflecting the equally evasive and

[8] See Data Act's Undue Data Portability Restrictions: CCIA Requests EU Privacy and Competition Enforcers To Step In, CCIA Europe (June 2023), https://ccianet.org/news/2023/06/data-acts-undue-data-portability-restrictions-ccia-requests-eu-privacy-and-competition-enforcers-to-step-in/

non-binding language of Recital 40.[9] However, neither the Commission's interpretation of Article 5(2), nor recital 40 resolve the inherent conflict.

User portability rights under the GDPR and DMA are binding statutory obligations, not some voluntary business arrangements. Article 5(2) contains no textual exception for user-initiated transfers, and neither the non-binding language of a Recital nor administrative guidance can rewrite the plain language of the law. Furthermore, companies cannot defend enforcement actions by citing a Commission FAQ that contradicts the statute they may be charged with violating.

Beyond the administrative burden, this incoherence actively undermines the EU's competitiveness agenda. By effectively blocking consumers from transferring their data to the service provider of their choice, the current framework inadvertently fosters lock-in and nullifies the individual's control over their personal data. To deliver genuine simplification and legal certainty, the Omnibus must establish a definitive hierarchy of norms. It must be made clear that industrial policy restrictions in the Data Act cannot supersede the fundamental right of users to freely port their data.

**Call to action:** Co-legislators should introduce a targeted amendment clarifying that the exclusion of gatekeepers in Article 5(2) of the Data Act is without prejudice to, and does not restrict, the exercise of user-initiated data portability rights under the GDPR or the DMA.

## 8. Harmonise DPIAs and enforce 'One Assessment' principle across laws

CCIA Europe supports the Commission's proposal to create a single, harmonised EU-wide list of processing operations requiring a data protection impact assessment (DPIA) under Article 35(4), replacing the current patchwork of 27 national lists. Harmonisation must mean genuine simplification, however, not a compilation of every Member State's strictest requirements. The Omnibus should thus mandate that the harmonised list reflects consensus on genuinely high-risk processing, not an accumulation of all possible risks.

The current proposal also fails to address a practical impossibility: applying new DPIA requirements to existing products. Article 35 requires assessments "prior to processing," so strictly applying new lists to services operating safely for years would create retroactive non-compliance. A grandfathering provision is essential to ensure new DPIA obligations apply only to new processing operations.

Finally, true simplification requires addressing definitional misalignment across the EU's digital rulebook. 'Automated decision-making' means different things under GDPR Article 22, the AI Act, and the Platform Work Directive – creating overlapping obligations and fragmented oversight. Businesses face duplicative reporting to data protection authorities, AI regulators, and labour authorities for the very same technology. The Omnibus should operationalise a 'assess once, comply many' approach by clarifying that a comprehensive DPIA under GDPR automatically satisfies related requirements under other EU acts,

[9] See Frequently Asked Questions on the Data Act, section 36, version 1.4 (January 2026), https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act, and and last sentence of Recital 40 Data Act: "As voluntary agreements between gatekeepers and data holders remain unaffected, the limitation on granting access to gatekeepers would not exclude them from the market or prevent them from offering their services."

including the AI Act's Fundamental Rights Impact Assessment and the Platform Work Directive's reporting obligations for automated monitoring systems.[10]

**Call to action:** The Omnibus proposal should specify that the harmonised DPIA list must reflect risk-based consensus, not an amalgamation of all national requirements. A grandfathering provision would also ensure new DPIA requirements apply only to processing operations initiated after entry into force. The Regulation should also clarify that a GDPR DPIA satisfies the assessment obligations under other Union law, specifically the Fundamental Rights Impact Assessment (FRIA) under the AI Act and the reporting requirements for automated systems under the Platform Work Directive, to eliminate administrative duplication.

## III. Harmonising cybersecurity compliance

*The proposed single-entry point for incident reporting is a good first step. Yet, online interfaces alone cannot solve fragmentation if timelines, thresholds, and templates still differ across the GDPR, NIS2 Directive, Cyber Resilience Act (CRA), and the Digital Operational Resilience Act (DORA).*

### 9. Ensure 'single-entry point' integration and industry consultation

CCIA Europe supports establishing a single-entry point managed by the European Union Agency for Cybersecurity (ENISA) to unify incident reporting under NIS2, GDPR, CRA, DORA and other acts. However, Article 23a(1) of the amended NIS2 Directive uses insufficient language to deliver meaningful simplification. Indeed, it merely states that ENISA "may" ensure the single-entry point builds upon the Cyber Resilience Act (CRA) platform, leaving room for fragmentation where manufacturers toggle between one portal for product vulnerabilities (CRA) and another for operational incidents (NIS2). The Omnibus should mandate technical unification, ensuring full backend integration rather than theoretical alignment.

The governance structure for designing the single-entry point also needs improvement. Article 23a(3) requires ENISA to develop technical specifications and API standards with the Commission, CSIRTs network, and competent authorities. But it noticeably excludes reporting entities themselves. Excluding primary users from the design phase risks creating a system that works for regulators but proves operationally incompatible with enterprise security workflows. Given the single-entry point must interoperate with European Business Wallets for authentication, industry stakeholders must be formally consulted on technical architecture to ensure APIs are robust, secure, and fit for purpose.

**Call to action**: Co-legislators should amend Article 23a(1) of the NIS2 Directive to change "may ensure" to "shall ensure," guaranteeing that the single-entry point is technically integrated with the Cyber Resilience Act reporting platform to prevent the proliferation of disconnected portals. Additionally, Article 23a(3) should be amended to explicitly include 'reporting entities' or industry stakeholders in the list of parties ENISA must consult when

[10] Misalignment in the regulation of automated systems was already identified by CCIA Europe in our position paper prior to the digital Omnibus proposal being published, see p.8 here: https://ccianet.org/wp-content/uploads/2025/10/CCIA-Europes-Position-Paper-on-the-European-Commissions-Digital-Simplification-Efforts.pdf

developing technical specifications and API standards. Lastly, the Regulation should introduce a formal mechanism for entities to report operational bugs or technical failures within the single-entry point to ENISA, ensuring that technical outages do not result in unfair liability for missed reporting deadlines.

### 10. Establish a unified incident-reporting standard across laws

While establishing a technical single-entry point managed by ENISA is a welcome step, it risks becoming a mere digital postbox for legal requirements that would continue to remain fragmented. The Omnibus leaves distinct and conflicting reporting rules intact, creating a paradox where entities must report via one tool but track different countdown clocks for the same event: 24 hours under NIS2's 'early warning', 72 hours under standard practice, and now 96 hours for high-risk GDPR breaches. This lack of substantive harmonisation diverts resources from actual incident response towards complex administrative assessments of which legal threshold applies to each regulator.

To achieve genuine 'report once, share many' co-legislators must harmonise the underlying rules, not just the interface through which companies are expected to submit their reports. This requires standardising the reporting clock around a single deadline and aligning the trigger point so obligations arise only when an incident is confirmed rather than merely suspected, preventing precautionary over-reporting that floods authorities with noise. The Commission should also mandate a harmonised reporting template across all acts covered by the single-entry point (building on DORA's experience) ensuring entities submit one unified report rather than filling disparate forms within a single portal.

**Call to action:** Lawmakers should seize the chance of this Omnibus to standardise reporting timelines around a single 72-hour deadline for all regulations covered by the single-entry point (aligning NIS2, DORA, and GDPR), and to ensure alignment around reporting thresholds. This should include language which explicitly starts the reporting clock when an incident is confirmed, not when merely suspected or detected. It should also include harmonisation of definitions of 'high risk' (GDPR) and 'significant incident' (NIS2) via implementing acts to ensure consistent severity assessments. Finally, co-legislators are encouraged to mandate a harmonised reporting template across the acquis. For Article 33 GDPR the EDPB template should be fully aligned with the single-entry point logic and DORA standards.

## Conclusion

The Digital Omnibus offers a unique opportunity to pivot from a period of intense but uncoordinated EU regulatory output to one of pragmatic implementation. By modernising data protection rules to adapt to new technological realities and jurisprudence, rejecting new complexities like browser-based consent, resolving conflicts between the Data Act and other flagship EU legislation, and harmonising the underlying logic of cybersecurity reporting, this Digital Omnibus proposal can genuinely contribute to building a better digital rulebook that is actionable and predictable.

CCIA Europe stands ready to support the European Commission, the EU Council, and the European Parliament in refining and grounding this proposal in operational reality, delivering meaningful simplification while strengthening user safeguards.

# About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009. CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

Visit ccianet.eu, x.com/CCIAeurope, or linkedin.com/showcase/cciaeurope to learn more.

## For more information, please contact:

CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org