Council of the European Union
General Secretariat

PUBLIC

Brussels, 30 April 2026

WK 6156/2026 INIT

LIMITE

SIMPL	**TELECOM**
ANTICI	**CODEC**
DATAPROTECT	**PROCIV**
CYBER	**COMPET**
	MI

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Antici Group (Simplification)
Subject:	Omnibus VII (Digital Omnibus): Explanatory note on Cyber and Data accompanying the Presidency's revised compromise text

Delegations will find enclosed an explanatory note accompanying the Presidency's revised compromise text (doc. ST 8261/1/26 REV 1) for the Antici Group (Simplification) meeting on 8 May 2026 on Omnibus VII (Digital Omnibus) in relation to cyber and data components.

Explanatory note

In view of the AGS meeting of 8 May 2026, this explanatory note highlights and explains the main changes proposed concerning the cyber/single-entry-point provisions. Further details on the changes in relation to the Data acquis and cyber/single-entry point provisions are included in the annexed Explanatory Table. This document is for reference only.

PUBLIC

Cyber related provisions / Single-entry-point
Articles 6 to 9, Recital 49 to 57.

The Presidency took note of the strong reservations and opposition from several delegations regarding the possible establishment of a single-entry point for incident reporting at EU level, citing concerns in terms of further complexity for incident response and notification, as well as possible risks to the security of information systems and national security.

The Presidency considers however that there are converging views on the need to simplify the cybersecurity landscape and on the added value of the alignment and streamlining of incident notifications, which could directly contribute to regulatory simplification for the concerned entities.

Based on the discussions already held and the written contributions received, the Presidency considers that **a compromise might be reached by exploring alternatives to the initial Commission's proposal to establish a single-entry point for incident reporting at EU level**, **while supporting entities navigating the current regulatory landscape and simplifying the process to comply with their notification obligations.**

Given the above, the Presidency invites delegations to consider the following **compromise package to advance discussions further** on these provisions:

- Shifting from a centralized reporting point to an information hub at EU level: the Presidency suggests replacing the Commission's initial proposal to establish a single-entry point at EU level with a single-information point managed by ENISA, effectively serving as a dynamic, guided navigation tool that clarifies reporting obligations without storing or processing actual incident notifications.

- Establishing one national entry point in each Member State: as a first step towards the simplification of notification requirements, the Presidency proposes that Member States establish their own national entry point, taking into account their needs and existing structures, supported by ENISA-developed guidelines which may include technical specifications necessary to ensure interoperability.

- Working towards the harmonisation of incident notification: the Commission shall swiftly submit a report outlining common definitions, thresholds, deadlines, formats, and procedures, and considering concrete steps and a timeline for the introduction of a unified incident reporting approach. In parallel, ENISA shall develop harmonization guidelines, focusing on standardizing reporting templates, analysing and suggesting harmonization of sectoral thresholds, and streamlining notification stages.

- Fostering cross-border incident notification: Member States should aim at facilitating cross-border notification to national structures, supported by ENISA which shall harmonise its

relevant tools and facilitate an automatization process to exchange information about cross-border impacts.

➔ **Considering the positions expressed by delegations, the Presidency takes the view that this compromise package addresses the need to preserve existing structures while introducing a relevant and valuable first step for the simplification of the regulatory landscape for incident reporting.**

PUBLIC

Annex - Explanatory Table

The purpose of this explanatory table is to provide delegations with additional information, clarifications and reasoning for the amendments proposed by the Presidency. The explanatory table follows the order of the relevant provisions.

Recitals	
Data acquis	
Recital (8)	The addition aims for a clearer language. The deletion is necessary to clear up a clerical error.
Recital (11)	The addition aims for a linguistic clarification of the situation when the refusal of granting access to data is necessary because there is a risk of trade secret disclosure.
Recital (17)	The deletion is a linguistic clarification. Deleting the second part of the sentence is necessary as it has been replaced by the first part.
Recital (19)	Responding to the requests from Member States that the Commission should monitor the deviations.
Recital (22)	The first addition preserves the flexibility to maintain the various national administrative structures. The second amendment inserts language of Recital (54) of the Open Data Directive on the scope of intellectual property rights.
Recital (25)	The addition preserves the flexibility for the Member States to further specify the criteria in order to define a very large enterprise.
Recital (26)	The change reflects that open data are not exclusively held only by governments.
New Recital (26a)	In relation to Article 42, this new recital clarifies the nature of the role of EDIB and its method of working in subgroups.
Cyber / Single-entry-point	
Recital (49)	The recital is amended to algin with Presidency proposal under Article 6(2) establishing a national entry point for incident reporting.
Recital (49a)	New recital accompanying the Presidency proposal under Article 6(1) establishing a single information point at EU level.
Recital 50	The recital is amended to algin with Presidency proposal under Article 6(1) 2. establishing a national entry point for incident reporting, also referring to the development of guidelines by ENISA and the related technical, operational and organisational measures.
Recital 51	The recital is amended to algin with Presidency proposal under Article 6(1) 2. establishing a national entry point for incident reporting,
Recital 52	The recital is amended to align with the Presidency proposal under Article 6(1) 3. on the harmonisation of the incident notification framework.
Recital 53	The recital is deleted, as it refers to the establishment of the single-entry point as initially proposed by the Commission.
Recital 54	The recital is deleted, as it refers to the establishment of the single-entry point as initially proposed by the Commission.
Recital 55	The recital is amended to algin with Presidency proposal under Article 6(2) establishing a national entry point for incident reporting.
Recital 56	The recital is amended to algin with Presidency proposal under Article 6(2) establishing a national entry point for incident reporting.
Recital 57	The recital is amended to algin with Presidency proposal under Article 6(2) establishing a national entry point for incident reporting.

PUBLIC

Articles	
Data acquis	
Article 1.1(a)(ed)	Supporting simplification effort by removing the rules on requesting data in public emergencies and where there is an exceptional need, given the continuing uncertainty surrounding the application of these rules.
Article 1.1(b)	Clarification in point (g) in order to refer to data only. Deletion of points (g) and (i) aims to avoid duplication: the scope of this chapter is repeated in Article 32i.
New Article 1.1(ca)	Clarification to ensure that these provisions do not create a legal basis for processing and are without prejudice to the application of the GDPR.
Article 1.1(13)	Clarification to enhance clarity on the minimum harmonisation requirement, as stated in Recitals (17) - (19) of the Open Data Directive.
Article 1.2(a)(4b)	The aim of this addition is to clarify that this definition of "permission" is used in the context of Chapters VIIa and VIIc only, as the same concept is used in e.g. Chapter II in a different context.
Article 1.2(a)(4c)	The deletion of the definition from the Data Governance Act is aimed to avoid uncertainty in the context of Chapter II the Data Act.
Article 1.2(b)	The definition in Article 2(10) of the Data Act is replaced and clarified. At the same time, it is deleted from point (38a).
Article 1.2(b)(28a) and (28(b)	To provide for legal clarity, the definitions are now taken over from the Public Procurement Directive. As a consequence, points (a)-(c) are deleted in both paragraphs.
New Article 1.2(b)(f)	The definition is aligned with Article 2(1)(b) of the proposal as regards digitalisation and common specifications (Omnibus IV).
Article 1.2(b)(f)(49)	The addition is to clarify that this definition is valid in the context of re-use of public sector data.
Article 1.2(b)(f)(50) and (51)	The addition is to addresses concern that digitised documents are always data, while „documents" captures non-digital elements, too.
Article 1.2(b)(f)(52)	While high-value datasets are digitised by definition, the deletion ensures that there is no obligation to digitize documents to make them available.
Article 1.2(b)(f)(56)	The deletion of "file" aims to reflect that, in practice, data are often shared not in files but via APIs.
Article 1.2(b)(f)(57)	The deletion reflects that files in open format are data by definition.
New Article 1.2(b)(f)(61)	The definition is aligned to Article 3(3) of Regulation (EU) 2018/1807 on free flow of non-personal data.
Article 1.4	To increase clarity on the application of this provision, the Commission, after consulting the EDIB, is now required to issue guidance.
Article 1.7.1 and 3.	The deletion of "mitigating" aims to avoid legal ambiguity.
Article 1.7.2.	The change of terminology aims to avoid legal uncertainty.
Article 1.7.9(b)iii	The change requires Union bodies, too, to notify EDPS in case of a request for personal data.
Article 1.7.9. new (ba)	This paragraph contained a reference to Art 15 which has been updated to Art 15a.
Article 1.7.11 new (aa)	This addition addresses concerns that Article 19 (1)(c) relates to documents and that the sense would be changed due to the insertion of a definition of document caused by the integration of the Open Data Directive. Consequently, in the last part of the paragraph, "public

	access to documents" has been changed to "public access to information".
Article 1.7.14(b)(c) and (d)	Editorial error corrected.
Article 1.7.15.1b and 1c	The first sentence of sub-paragraph 1b is separated as 1c, as it is more general and is not limited to SMEs and SMCs. In addition, reference to "services other than those referred to in Article 30(1)" is deleted, because there would be no justification for depriving IaaS providers from being able to impose early termination penalties.
Article 1.18, Article 32c(b)	The addition includes the detection of fraud and cybersecurity into the possible use of the intermediation service.
Article 1.18, Article 32c(d)	The amendments clarify that the services provided by the data intermediation service providers can be more and different than value added services.
Article 1.18, Article 32c(d)(i)	This change in point (i) clarifies that it refers to the clients of the data intermediation service providers and not to "users" in the sense of the Data Act.
Article 1.18, Article 32c(f) and (g)	Article 12(f) and (o) of the Data Governance Act.
Article 1.18, Article 32c new last sentence	The requirements (i), (ii) and (v) can be requested from micro and small enterprises without overburdening them. Requirement (iv) is not relevant to these companies, whereas (iii) would mean an unreasonably high burden on these companies.
Article 1.18, Article 32e(4)	The addition increases the flexibility for the competent authority by enabling the suspension and the duly substantiated extension of the time limit.
Article 1.18, Article 32g(1)	The addition reinserts Article 14(1) of the Data Governance Act, making the deleted text in the first sentence superfluous.
Article 1.18, Article 32g(5)	The addition at the end of the paragraph is necessary as the competent authority cannot remove an entity from the public Union register.
Article 1.18, Article 32i(4)	This clarification is a reinsertion of Article 1(2) of the DGA.
Article 1.18, Article 32k(1)(b) and (5)	The additions clarify that exclusive rights can be granted by contracts and administrative acts alike.
New Article 1.18, Article 32la	The purpose of this new Article is to harmonise the procedure, timeline and redress for requests for re-use of data held by public sector bodies. Article 32o is deleted.
Article 1.18, Article 32m	The addition contains a transparency obligation for public sector bodies.
Article 1.18, Section 2 title and Article 32q title	The change reflects that public sector data is not held only by governments.
Article 1.18, Article 32p(1)	The changes align the text to the new definition of documents as non-digitised content and the absence of an obligation to digitise documents.
Article 1.18, Articles 32q(6) and 32y(2)	The changes keep the flexibility for the Member States to set higher charges for re-use by very large enterprises, while reflects that these charges, in some Member States, are not set by the public sector bodies.
Article 1.18, Article 32r(3) and (4)	These standard licences obligations apply to public undertakings as well.
Article 1.18, Article 32s(2)	The wording has been changed to better reflect the language of a regulation.

Article 1.18, Article 32v(1)	High value datasets cannot be documents.
Article 1.18, Article 32v(5)	The deletion is part of the simplification effort. This provision was rarely applied and offered little margin for public sector bodies to continue charging.
Article 1.18, Article 32w(3)(ii)	This subpoint has been deleted to avoid uncertainty over the definition of "other forms of preparation".
Article 1.18, Article 32w(5)(a)	This subpoint has been deleted with the same Article paragraph (2)(c) in view.
Article 1.18, Article 32z(2) and (3)	The changes maintain the flexibility for the Member States in organising the operational aspects of their SIPs.
New Article 1.18a, Article 37(1)(a)	The addition is to clarify the Chapters VIIb and VIIc do not have competent authorities for enforcement.
New Article 1.18a, Article 37(1)(b)	The addition clarifies that authorities responsible for enforcement of the GDPR shall be responsible under this regulation for the enforcement of GDPR-related issues only, and not for enforcement of the rest of the provisions.
New Article 1.18a, Article 37(1)(c)	The addition provides for a legal basis for the exchange of information and cooperation between the competent authorities.
Article 1.18a, Article 38 new (4)	This paragraph has been reinserted from the Data Act.
Article 1.18a, Article 38 new (5)	The addition clarifies the relationship between Chapter VIIc and Article 38.
Article 1.22, Article 41a (1) and (2)	The additions emphasize the strategic nature of EDIB and provides for maintaining its thematic subgroups.
Article 1.23, Article 42(1) new (e), (f) and (g)	Chapters VI and VIII are not contained in the list of responsibilities of EDIP, as it would not be consistent with its other responsibilities and strategic nature.
Article 1.26, Article 49(a)(ia)	This paragraph contained a reference to Art 15 which has been replaced by Art 15a. This reference is updated.
Article 2, Article 11	The separate, prolonged period for entering into application for Chapter VIIc reflect the need for time to adapt national legislations.
Cyber / Single-entry-point	
Article 6(1)	The proposed new Article 23 is amended, replacing the initial Commission's proposal to establish a single-entry point by the establishment by ENISA of a single-information point for incident reporting. (Article 23, paragraphs (2) to (6), as initially proposed by the Commission are therefore deleted)
Article 6(1) 1a.	A new paragraph 1a. clarifies the main characteristics and elements of the single-information point, including the information to be provided to enable the identification of applicable obligations to report incident, as well as requirement in terms of navigation and availability of simplified and guiding information.
Article 6(1) 1b.	A new paragraph 1b. requires ENISA to consult relevant national competent authorities and others bodies (NIS Cooperation Group and CSIRT Network) when developing the single-information point, and mandate the establishment of structured communication channel for Member States to communicate to ENISA all relevant and necessary information.
Article 6(1) 1c.	A new paragraph 1c. clarifies that the single-information point serves only as an informational resource and cannot accept, store, or

	process actual incident notifications or collect identifying information about notifying entities.
Article 6(1) 1d.	A new paragraph 1d. requires ENISA to pilot the system within 12 months of the regulation's entry into force to ensure it meets the specific requirements of each applicable Union legal act.
Article 6(1) 1e.	A new paragraph 1e. tasks ENISA to provide a report, exploring the possibility to extend the single-information point
Article 6(2)	A new Article 23b requires Member States to establish and maintain national entry points for incident reporting under relevant EU legal acts, considering national needs and existing structures. ENISA is tasked with developing guidelines—consulting the CSIRTs network and Cooperation Group—to support Member States in establishing, maintaining, and securely operating their national entry point, addressing technical, operational, and organizational measures while ensuring interoperability across the Union. The guidelines may also enable entities to retrieve and supplement previously submitted information, and allow single submissions to fulfill multiple reporting obligations.
Article 6(3)	A new Article 23c mandates the European Commission to submit a report within six months of the regulation's entry into force, outlining common definitions, thresholds, deadlines, formats, and procedures across the relevant EU legal acts, in order to consider concrete steps and a timeline for the introduction of a unified incident reporting approach. Member States shall cooperate with the CSIRT network to enhance the exchange and interoperability of notification information, aiming to improve efficiency and consistency. Building on the Commission's report, ENISA must develop harmonization guidelines in cooperation with the NIS Cooperation Group, focusing on standardizing reporting templates, analyzing and suggesting harmonization of sectoral thresholds, and streamlining notification stages.
Article 6(4)	A new Article 23d on cross-border incident notification requires ENISA, working alongside the NIS Cooperation Group and the CSIRT Network, to develop and maintain mechanisms to facilitate the alignment of incident notifications submitted via Member States' national entre point with cross-border reporting obligations. It is clarified that information submitted trough relevant tools shall not be automatically transmitted to ENISA in full and that Member States shall have the possibility to select information shared.
Article 6(2)	Article 23 is amended to align with the Presidency proposal under Article 6(2) establishing a national entry point for incident reporting, and to cross-reference ENISA's task to provide a mapping of all competent authorities and CSIRTS.
Article 6(3)	Article 24 is amended to align with the Presidency proposal under Article 6(2) establishing a national entry point for incident reporting.
Article 7	Regulation (EU) 910/2014 is amended to align with the Presidency proposal under Article 6(2) establishing a national entry point for incident reporting.
Article 8	Regulation (EU) 2022/2554 is amended to align with the Presidency proposal under Article 6(2) establishing a national entry point for incident reporting.

Article 9	Regulation (EU) 2022/2557 is amended to align with the Presidency proposal under Article 6(2) establishing a national entry point for incident reporting.

PUBLIC