Council of the European Union
General Secretariat

Interinstitutional files:
2025/0360 (COD)

Brussels, 11 June 2026

WK 8070/2026 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:	Presidency
To:	Antici Group (Simplification)
Subject:	Omnibus VII (Digital): Presidency note - AGS meeting on 15 June 2026

In view of the AGS meeting on 15 June 2026, delegations will find enclosed the Presidency note, including the explanatory table on the revised Presidency compromise text, to provide delegations with additional information, clarifications and reasoning for the amendments proposed by the Presidency regarding the Digital Omnibus.

Presidency Note

The fourth Presidency compromise text (**ST 10426/2026**) builds upon the discussions held within the Antici Group on Simplification (AGS) on 27 May 2026, written comments received from delegations and takes into account the guidance for further work on the basis of the discussion held in Coreper on 8 June 2026.

The text addresses all provisions related to the Data Act, P2B Regulation, GDPR, ePrivacy Directive, and Cyber. The proposed amendments to the EUDPR are aligned with the compromises reached on the GDPR provisions. As such, this text incorporates and consolidates all elements of the Digital Omnibus Proposal.

The Presidency aims to use this Presidency Note as a basis for discussion in the Antici Group on Simplification on 15 June 2026. Furthermore, this note explains the rationale underlining various matters, that have either been amended or have not been further pursued in the development of discussions. Further details on the proposed changes are included in the annexed Explanatory Table. This document is for reference only.

In view of the AGS meeting of 15 June 2026, the Presidency proposes the following order of discussions on the entire compromise text.

Round 1: Data Act
The Presidency will hold a discussion concerning ECB relevant Articles. The Presidency will invite delegations to express their overall position on all provisions related to the Data Act, including the change proposed on trade secrets.
Round 2: P2B Regulation
The Presidency will inform delegations of minor adjustments made to Article 10 and invites delegations to express their overall position.
Round 3: Cyber provisions
The Presidency will present the updates made to the compromise text and invite delegations to express their overall position, with a particular focus on the proposed Article 23b establishing the national entry point.
Round 4: Application of pseudonymisation and identification of a natural person
The Presidency will invite delegations to express their positions in a constructive manner and provide concrete feedback on the updated proposal for a new Article 29a on pseudonymisation.
Round 5: Other GDPR provisions
The Presidency will invite delegations to express their positions and provide guidance on all other elements of the Presidency compromise text, as outlined in the following sections.
Round 6: Cookies and ePrivacy provisions
The Presidency will invite delegations to express their overall position on all provisions related to cookies and the ePrivacy Directive.

1. Data Act and data acquis

The Coreper guidance for further work indicated the need to increase the level of protection of trade secrets, with reference to Article 4 (8) of the Data Act. The Presidency therefore suggested additional amendments to Article 1(3) and 5(11) of the Data Act, with a view to alleviate applicable conditions while keeping the balance between protecting trade secrets and providing sufficient amount of data for innovation.

Apart from these amendments, the consolidated compromise text for discussion integrates the text circulated on 29 May 2026 (**ST 9845/2026**) without any further changes.

With reference to the non-paper circulated by Germany on 10 June 2026, the Presidency notes that the proposals were submitted at a very late stage of the discussions and outside the procedure followed by other delegations for the submission of comments and drafting suggestions. This has made their assessment more challenging within the available timeframe. The Presidency has carefully considered the proposals submitted and appreciates this constructive engagement in the discussions. Nevertheless, in the interest of transparency and inclusiveness, the Presidency has examined the proposals received by e-mail. However, the Presidency is not in a position to take these proposals on board.

As a general consideration, the Presidency recalls that the Digital Omnibus is intended as a targeted simplification exercise. Its objective is to reduce unnecessary administrative burdens, improve implementation and enhance legal certainty, while preserving the policy choices, institutional arrangements and regulatory balance established in the underlying legislation.

The Presidency considers that a significant number of the proposed amendments would go beyond simplification and would instead reopen substantive elements of the Data Act, the Open Data framework and the Data Governance Act. In several instances, the proposals would require a broader policy assessment, including consideration of their impact on users, public authorities, data holders, market participants and the overall functioning of the European data economy. The Presidency further notes that a number of the proposed amendments would affect core elements of the existing framework, including transparency obligations, enforcement mechanisms, supervisory arrangements and the balance of rights and obligations established by the co-legislators. Such changes cannot be regarded as purely technical or simplification-oriented in nature.

→ **The Presidency considers that the compromise text proposed meets the objective of consolidated and simplifying the legal framework fostering the use of data in the digital economy, while maintaining the necessary balance between the protection of trade secrets and the sufficient availability of good quality data in support of innovation, in particular AI development. Delegations will be invited to express their views on the overall compromise proposed for these provisions.**

→ **Against this background, the Presidency considers that these issues would be more appropriately examined in another legislative context and should not be pursued within the framework of the Digital Omnibus. The Presidency therefore considers that the current compromise remains the most balanced approach to delivering targeted simplification while preserving legal certainty, regulatory coherence and the integrity of the underlying legislative framework.**

2. P2B Regulation

Following the discussions held during the AGS meeting of 27 May 2026, the Presidency has maintained the compromise text proposed for the provisions related to the P2B Regulation.

As a technical adjustment, Article 18(1) is maintained in force, to ensure that the remaining articles of the P2B regulation are reviewed regularly, every 3 years.

→ **The Presidency considers that, with the inclusion of this adjustment, the compromise proposed reflects the views expressed by delegations, achieving the simplification objective and avoiding provisions overlap with other applicable frameworks, while maintaining relevant provisions of the P2B Regulation. Delegations will be invited to express their views on the overall compromise proposed for these provisions.**

3. Cyber

Following up on the Coreper guidance, the Presidency has introduced further modification to the proposed compromise, also based on contribution made by delegations, prioritizing operational flexibility and facilitating support and guidance in the establishment of national incident reporting entry points.

While Article 23a on the incident reporting information point has been further streamlined to maintain core information element, the restructuring of Article 23b introduces a flexible tiered approach for Member States to establish their national entry point, distinguishing between "core tasks" to be considered and integrated, and optional additional functions the national entry point may carry out. Crucially, the compromise text maintains that Member States retain the autonomy to configure their national entry points according to their national structures while simultaneously endeavouring to ensure interoperability with other national entry point.

With a view to further support Member States if they consider it necessary, Article 23b has also been updated to include a paragraph mandating ENISA, in cooperation with Member States, to develop an open-source solution that may be used by Member States in setting up their national entry point.

In line with delegations' comments, the Presidency has also updated the wording of the proposed Article 23c on harmonising incident notification framework and Article 23d on cross-border incident notification.

→ **The Presidency considers that the updated comprehensive echoes the call for further flexibility in the establishment by Member States of their national entry point, while maintaining the trajectory towards a simplified and efficient mechanism for incident reporting.**

4. GDPR and cookies

The Presidency acknowledges that in the last AGS meeting and during the Coreper discussion, some delegations have voiced concerns on whether the compromise text can deliver in response to the Proposal's simplification objectives. In response, the Presidency would like to highlight that the compromise text includes a series of simplification measures amending the GDPR, building upon the Commission proposal, as well as on additional proposals made by delegations during the discussions over the past 6 months:

- A common definition of scientific research.
- Compatibility of further processing for scientific research purposes without additional requirement.
- Exemption from information obligations for the further processing for scientific research purposes.

- Exemption from information obligations where there are reasonable grounds to assume that the data subject already has the information and the processing is not likely to result in a high risk.
- New derogation to the prohibition of processing of sensitive personal data for the purpose of biometric verification.
- New derogation to the prohibition of processing of sensitive personal data in the context of the development of AI systems.
- Dedicated article on the application of pseudonymisation, building upon CJEU case law and supporting controllers through consistent interpretation and guidance.
- Clarification that processing of personal data in the context of the development of an AI system or of an AI model can be carried out for the legitimate interest of the controller.
- Clarification and insertion of new criteria to support the assessment of excessive data subject requests by the controller.
- Clarification and insertion of new criteria to support the assessment of excessive data subject complaints by the data protection authority.
- Inclusion of processors under the scope of Article 25 GDPR on data protection by design and by default.
- Removal of the obligation to notify the contact details of the data protection officer to the data protection authority.
- Obligation to notify data breaches limited to breaches likely to result in a high risk and extension of the deadline for notification from 72 to 96 hours.
- Common template for the notification of data breaches and the carrying out of a data protection impact assessment.
- Single list at EU level of processing likely to result in a high risk for data subject (instead of 27 lists) and single list of processing not likely to result in a high risk for data subject.
- Additional guidelines by the EDPB on key provisions in support of controllers' compliance and clarification for a more consistent application of data protection authorities' interpretation.
- Single framework for the rules applicable to cookies and additional exemptions from consents, including for audience measurement and fraud prevention, thus significantly reducing the number of cookies banners online.

Throughout technical discussions, and at Coreper level, delegations raised concerns regarding the scope of the proposed GDPR simplification measures and indicated that they require additional time to reflect on the entire proposal, given its complexity and potential implications.

The Presidency also notes that the absence of an impact assessment has added to the challenges encountered during the examination of the proposal. A significant number of delegations highlighted this concern throughout the discussions, particularly when considering amendments affecting fundamental GDPR concepts, such as the definition of personal data and the rules relating to cookies and similar technologies.

The Presidency compromise seeks to deliver targeted simplification while preserving legal certainty, consistency with the GDPR framework, and the protection of fundamental rights. In the Presidency's view and as expressed by many delegations, simplification should not lead to substantive revisions of the core principles and concepts of the GDPR. The current text aims to strike a proportionate balance between reducing administrative burdens and ensuring the effective and coherent application of the existing framework. More far-reaching amendments

could risk creating legal uncertainty for both competent authorities and stakeholders, without demonstrating clear additional benefits in terms of simplification.

→ **In the Presidency's assessment, discussions have demonstrated need for caution when considering changes that could have broader consequences, not only for data subjects, but also for companies and the digital economy, extending beyond the targeted simplification objectives of this initiative.**

→ **The Presidency considers the balance that should be drawn between the substantial depth of amendments and the framework in which discussions take place, and considers that the compromise text strikes such balance, delivering concrete simplification gains while maintaining a high level of data protection.**

Application of pseudonymisation and identification of a natural person
Article 3(1), Article 3(10) – Proposed Article 29a GDPR, Recital 27a, Recital 27b

To answer Member States' demands of further clarifying pseudonymisation in the operative part of the GDPR, while at the same time acknowledging the requests of Member States to not alter Article 4(1) GDPR, the Presidency has proposed Article 29a. In its fourth compromise text, the Presidency has updated Article 29a to reflect concerns around the need for more ambition and further integration of relevant case law and of the consequences of the application of pseudonymisation, in support of data controllers' compliance.

The Presidency acknowledges views of a few delegations to alter the definition of personal data under Article 4(1) GDPR, which have been apparent since the beginning of discussions. The Presidency reiterates that, in line with most recent CJEU case law, pseudonymisation does not belong to the definition of personal data. The Presidency refers to the application of pseudonymisation under Article 29a in a manner which preserves the essence of pseudonymisation as a measure of data protection, as already prevalent in the GDPR.[1]

The Presidency recognizes that a subjective definition could create simplification and alleviate companies from compliance with various obligations towards data subjects. However, introducing a subjective definition of personal data within a fundamental rights legislation would also shifting the assessment of whether data is personal towards specific capabilities and organisational arrangements of a particular entity, thus also fragmenting the application of the GDPR in the digital economy. As various delegations have outlined, such an approach may weaken existing safeguards, raise enforcement and accountability concerns, and declare supervisory assessments considerably more complex. The Presidency therefore echoes most views expressed in maintaining the deletion of the amendment to the definition of personal data in all compromise texts.

The current text requires the EDPB to issue an Opinion on the application of pseudonymisation and anonymisation referred to in Article 29a, in accordance with Article 64 GDPR. The Presidency throughout the discussions has considered majority of delegations' views to attribute power to the EDPB, instead of mandating the Commission to adopt implementing acts, but aimed to enhance this power by incorporating the adoption of an Opinion instead of guidelines. The involvement of the European Data Protection Board is not intended to shift

[1] Recital (28) GPDR; The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

legislative competence, but to ensure uniform interpretation and technical consistency, in line with its existing mandate under Article 64 GDPR. This ensures that guidance is developed in a coherent manner, reflecting both technological realities and the need for legal certainty.

Contrary to guidelines, the adoption of an opinion would further anchor the provided guidance within the GDPR consistency mechanism, thus addressing fragmentation concerns. The Presidency recalls that, in line with the GDPR and related case-law, although the proposed opinion has no direct binding effect on controllers or national supervisory authorities, it ensures more robust and consistent interpretative guidance, which may ultimately lead to a binding decision by the Board in a particular case[2].

Paragraph 2 of the updated Article 29a now fully anchors in the operative part of the GDPR the main elements of the CJEU ruling in the SRB case, clarifying that the application of pseudonymisation may effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable.

In this light, the Presidency considers that Article 29a constitutes a targeted clarification measure, reinforcing legal certainty and operational usability of pseudonymisation within the GDPR, without modifying the core definition of personal data.

→ **The Presidency considers that the newly introduced Article 29a provides necessary added value to controllers and processors regarding the application of pseudonymisation and addresses the gap that exists in clarifying how compliance with GDPR obligations can be achieved through the measure of pseudonymisation.**

→ **The Presidency considers that keeping the definition of personal data untouched preserves legal certainty, ensures consistency across EU legislation, and avoids reopening settled GDPR concepts.**

→ **The Presidency considers that the solution of an EDPB Opinion could allow for more legal certainty instead of the issuing of guidelines.**

Personal data processing for purposes of AI Training
Article 88c

The Presidency carefully examined the proposed additions concerning specific safeguards applicable when personal data are processed for the development and operation of AI systems and AI models. While the Presidency recognises the objective of ensuring a high level of protection for data subjects, Article 88c has not been furthered for several reasons.

The proposed safeguards largely restate or further specify obligations that are already contained in the GDPR. Reiterating or elaborating on these obligations in this Regulation risks creating unnecessary overlap and legal uncertainty regarding the relationship between the two legal instruments.

[2] The consistency mechanism, like the rules on cooperation between supervisory authorities, provides for a non-binding advisory phase before the adoption, where appropriate and in relation to specific cases, of binding decisions of the EDPB. See paragraph 29 of Ordonnance, 29/04/2025, Meta Platforms Ireland / Comité européen de la protection des données, T-319/24.

Several delegations have emphasised the importance of preserving the technology-neutral and sector-neutral character of the GDPR. Introducing AI-specific examples or conditions in relation to the application of Article 6(1)(f) GDPR could be interpreted as creating a special regime for AI-related processing, thereby departing from the established framework of the GDPR and potentially prejudging how the legitimate-interest balancing test should be conducted in individual cases. The Presidency considers that the proposed wording may inadvertently alter the interpretation of existing GDPR obligations by suggesting that certain safeguards are specifically required when legitimate interests are relied upon in the AI context. This could create legal uncertainty both for controllers and for data subjects and may lead to divergent interpretations across sectors.

The Presidency recalls that highlighting of a particular lawful ground for processing in the operative part of the GDPR would risk undermining the principle of accountability and the approach followed by data protection authorities, based on the absence of hierarchy between the different lawful grounds for processing under Article 6 GDPR and the responsibility of controllers to determine the most appropriate ground on a case-by-case basis.

→ **The Presidency considers that Recital (33a) of the compromise text targets the objective of clarification, by exemplifying that the processing of personal data in the context of the development and deployment of an AI system or of an AI model, may be regarded as carried out for a legitimate interest of the controller, subject to relevant GDPR provisions. This approach follows already existing references to examples of legitimate interest within the GDPR.**

Data Breach Notifications
Article 8 – Recital 39

The Presidency in all compromise texts has so far maintained 72 hours, considering delegations views on maintaining a high-risk threshold, responding therefore to the earlier notification in the case that highly sensitive data are breached. However, considering demands by several delegations for further simplification efforts and the need for a more ambitious text, the Presidency has altered this threshold to 96 hours.

Information obligations
Articles 3(4) and 3(5) - Recitals 35, 35a, 36

The amendments submitted by delegations on Article 3(4), concerning Article 12(5) GDPR, contain proposed wording aiming to lower the burden of proof when refusing requests, by allowing controllers to rely on "reasonable grounds to believe" that a request is excessive or submitted with an abusive intention.

While the stated objective is to facilitate the practical application of the provision and alleviate the controller's burden, the Presidency notes that such an amendment would be impacting on the exercise of data subjects' right and does not correspond to the latest CJEU case law on the matter. The Presidency also flags that lowering the burden of proof for controllers could lead to divergent practices among controllers and supervisory authorities and increase disputes concerning the refusal of requests.

In addition, to address concerns regarding the complexity of the provisions as drafted and simplify its application, the Presidency proposes to restructure and streamline the addition of Article 13(5), laying down the circumstances to be met in order for the exemption from information obligations to apply.

→ **To ensure that proposals made by delegations are fully considered, the Presidency invites delegations to provide their preference regarding bracketed wording, in particular "[also, for request under Article 15] and "[that there are reasonable grounds to believe that it is excessive or submitted with an abusive intention, based on objective circumstances related to the request or the conduct of the data subject]".**

→ **The Presidency supports that the current text provides relevant, targeted and legally consistent simplification of Article 12(5) and, despite extensive discussion already held, will invite delegations to express their position, including on alternative wording proposed.**

→ **The Presidency in the current compromise text has further clarified the scope of Article 13(4) GDPR, in response to delegations' comments, with the aim to create a more comprehensive structure of the exemption from information duties.**

Cookies
Proposed Article 8a GDPR (now deleted), Article 5(2) and corresponding Recitals

After the discussion in Coreper on 8 June 2026, based on the delegations' views on the insufficiency of evidence on economic and human rights impact, as well as technical challenges posed, the Presidency has decided to delete the proposed Article 8a, originally Article 88b in Commission's Proposal, and corresponding recitals.

Regarding Article 5(2) and corresponding recitals, amending the list of purposes for which consent is not required for the placing of cookies under the ePrivacy Directive, the Presidency has considered delegations' points on the scope of the purposes outlined and has proceeded with finetuning the so-called "whitelist". Audience measurement has been further clarified and exemplified. An additional exemption has been added for the prevention of fraud, with specific safeguards

In addition, the Presidency has included further exemplification in corresponding recitals, including cases of maintaining or restoring the security of a service, and measures taken for the detection and prevention of fraud.

→ **The Presidency considers that rules for a centralized mechanism has been one of the elements of the Digital Omnibus that aimed for simplification in the benefit of users but however acknowledges the concerns of delegations and Coreper guidance that the lack of an impact assessment outlining potential consequences to fundamental rights and economic as well as other factors, cannot sufficiently inform positions at this stage.**

→ **The Presidency supports that the current text provides a clearly framed, coherent and comprehensive list of exemption from consent requirement, including for new purposes, which should thus significantly reduce the number of cookies banners online while preserving users' protection under a single legal framework.**

Automatic exchange of tax information
Spanish Non-Paper on Article 49 GDPR

The Presidency understands the concerns and constructive contribution raised by Spain in its Non-paper on Article 49 GDPR (**WK 5822/26**). As this amendment would facilitate the automatic exchange of tax information to third countries, the Presidency considers, after careful examination of this proposal, that such proposal should not be discussed within the Digital Omnibus exercise.

The Presidency maintains that the Digital Omnibus is intended as a targeted simplification exercise for the digital legal framework of the EU. Should delegations consider that further work is warranted, the Presidency remains open to discussing the issue in the most suitable forum and legislative context. The Presidency has taken note of the Commission's view as it was presented to delegations in the AGS meeting of April 2026, proposing the opening of channels with the EDPB to clarify the already existing guidelines.

→ **The Presidency considers that this matter should not be pursued within the framework of the Digital Omnibus, but through other, more appropriate, legal or policy avenues. As such, the Presidency will not further organise discussions on this matter.**

Annex - Explanatory Table

Recitals	
Data acquis	
Recital (15)	With reference to Article 15a, this text clarifies the scope of the measures and maintains the rule that data cannot be requested for preventive measures, before the public emergency is declared. It also clarifies that - since the notion of "mitigating" is covered by "responding to" - it is better to delete the term for enhancing the clarity of the provision.
Recital (22)	The added paragraph is a clarification contained in Recital (56) of the Open Data Directive.
Recital (24a)	The added new Recital is an introduction of Recitals (11) and (12) of the DGA. Though the Digital Omnibus does not amend the underlying rules, their addition clarifies the scope of Section 3 relating to the former rules of the DGA and is deemed important to clarify the interpretation.
Recital (26a)	There was some uncertainty of the extent of the responsibility of DPAs in the DA. This new Recital is a clarification as a consequence of the deletion of Articles 37 and 40. It clarifies the role of the supervisory authorities responsible for monitoring and enforcement of GDPR under the DA.
Recital (26b)	This Recital now clarifies that EDIB should continue to serve as a forum for competent authorities and specifies the chapters of the DA where the Board's role is to develop consistent practices for the competent authorities.
Recital (26c)	The recital clarifies that the right to lodge a complaint and the right to an effective judicial remedy does not apply to Chapters VIIb (free flow of non-personal data) and VIIc (re-use).
Recital 62	The recital makes clear that the reasons and policy objectives that led to the adoption of the rules of Data Governance Act, the Free Flow of non-personal Data Regulation and the Open Data Directive, and which are re-enacted in the Digital Omnibus, remain valid. This addresses the concern by Member States that not all Recitals of these instruments are being introduced in the Digital Omnibus.
GDPR and ePrivacy	
Recital 27	No changes compared to the previous compromise text.
Recital 27a	Wording updates and amendments to include a reference to "prohibition by law" and also refer to "processors" in relation to the EDPB Opinion.
Recital 27b	No changes compared to the previous compromise text.
Recital 28	Legislative drafting adjustments and inclusion of the situation where scientific research activities are "mandated and conducted by public authorities or private entities".
Recital 29	Wording updates.
Recital 30	No changes compared to the previous compromise text.
Recital 31	No changes compared to the previous compromise text.
Recital 32	No changes compared to the previous compromise text.
Recital 33	The recital has been amended to align with the wording of Article 9(2)(l) and to further clarify the possible technical and organisational measures to avoid the processing of special categories of personal data.

	Further wording adjustments ("limited to incidental and residual processing", "technical operation"). The acquisition or providing of data in replacement of sole input via prompts. Further exemplification of non-application of the derogation in relation to special categories of data has been included.
Recital 33a	Legislative drafting adjustments ("an appropriate lawful ground", "or where other Union or national laws") and deletion of already applicable provisions. Inclusion of the "legitimate interests of artists and creative professionals" in the context of processing of personal data based on legitimate interest.
Recital 34	The recital has been amended to avoid referring to the notion of "biometric recognition" and instead focus on the two distinct purposes for which biometric data may be processed. In addition, reference has been made to exemplify technical and organisational safeguards.
Recital 35	No changes compared to the previous compromise text.
Recital 35a	Aligned with terminology of Recital 35 and clarification of repeated requests based on CJEU case law.
Recital 36	Legislative drafting adjustments (alignment with "direct and clearly circumscribed relationship") and further exemplification of such relationship.
Recital 37	No changes compared to the previous compromise text.
Recital 38	No changes compared to the previous compromise text.
Recital 39	Deletion of reference to Article 30 GDPR and inclusion of reference to the list of processing activities not likely to result to a high risk.
Recital 39a	Legislative drafting adjustments.
Recital 40	No changes compared to the previous compromise text.
Recital 40a	Amendment to include a reference to the "repealing" of national relevant guidelines, recommendations and best practices when necessary.
Recital 41	No changes compared to the previous compromise text.
Recital 42	No changes compared to the previous compromise text.
Recital 43	No changes compared to the previous compromise text.
Recital 43a	No changes compared to the previous compromise text.
Recital 44	Correction to refer to "Directive 2002/58/EC" instead of "Regulation (EU) 2016/679".
Recital 44a	Alignment with wording of Article 5(3) ePrivacy Directive. Further clarification of examples and limitations with reference to the independent media measurement under the EMFA.
Recital 44b	Recital providing clarification and examples in relation to the whitelist under Article 5(3) ePrivacy Directive.
Recital 44c	Wording updates.
Recital 45	Wording updates.
Recital 46	Deleted in line with the deletion of Article 8a of the previous compromise text (Article 88b of Commission's proposal).
Recital 46a	Deleted in line with the deletion of Article 8a of the previous compromise text (Article 88b of Commission's proposal).
Recital 47	No changes compared to the previous compromise text.

Recital 48	No changes compared to the previous compromise text.
Cyber	
Recital 49	Wording updates to align with the changes made in Article 23a.
Recital 49a	Additional clarification on the information provided in the incident reporting information point.
Recital 50	Alignment with the changes made in Article 23b.
Recital 50a	Wording updates to include reference to CSIRT and other designated authorities.
Recital 50b	Wording updates to include a reference to further costs related to cross-border interoperability.
Recital 51	No changes compared to the previous compromise text.
Recital 52	No changes compared to the previous compromise text.
Recital 53	No changes compared to the previous compromise text.
Recital 54	This recital has been reinstated but aligned with the compromise proposal and the establishment of a national entry point.
Recital 55	Additional clarification on the information exchanged, remaining under the control of Member States.
Recital 56	Additional clarification with reference to possible new amendments of other Union legals acts and the date when the national entry point should be used
Recital 57	No changes compared to the previous compromise text.
Recital 58	No changes compared to the previous compromise text.
Recital 59	Updated to align with the operative part of the compromise text.
Articles	
Data acquis	
Article 1.2(ea), Article 2(39) Data Act	As the main provision on smart contracts has been deleted (Article 36), the definition should also be deleted.
Article 1.2(e), Article 2(50) Data Act	"Document" is deleted as the research data are made public through depositories and have been referred to in the Open Data Directive as "documents in digital form", which, under the new definition, would be "data".
Article 1.2(e), Article 2(51) Data Act	"Data" are added for the purpose of consistency.
Article 1.2(e), Article 2(52) Data Act	The text has been reverted to the original proposal containing "documents", too.
Article 1.3, Article 4(8) Data Act	The changes increase the level of the protection of trade secrets while keep the balance between protecting them and providing sufficient amount of data for innovation.
Article 1.3, Article 5.11 Data Act	Delegations requested that the Commission issue guidance, in consultation with EDIB, on certain aspects of the application of this paragraph.

Article 1.4, Article 11 Data Act and Article 1.18aa(a), Article 33.1(d) Data Act	The amendment contains the deletion of the reference to smart contracts as an example. It is a consistent change following the deletion of Article 36 Data Act and the definition in Article 2(39) Data Act. The same reasoning applies to the change in Article 33 (1)(d) Data Act.
Article 1.7, Article 15a.1 Data Act	Deletion of "exceptional" to ensure legal clarity and that the right to request data regarding public emergencies will not be interpreted narrower than under the current Chapter V text.
Article 1.16, Article 32 Data Act	No changes are introduced since national criminal law is understood to be part of national law, with which transfer of or access to non-personal data can create a conflict.
Article 1.18, Title of Chapter VIIa	The added text increases legal clarity.
Article 1.18, Article 32c Data Act	"Data user" is added as it is one of the various categories of data-sharing stakeholders in the current DGA.
Article 1.18, Article 32c(h) Data Act	The deletion of the reference to point (d)(iv) in the last sentence makes clear that if a micro/small-sized enterprise becomes a gatekeeper, it is also excluded from obtaining the label. In other words, micro/small-sized enterprises are only exempted from the requirement of "functional separation".
Article 1.18, Article 32e.2 Data Act	The addition clarifies that these points refer to how to designate the competent authorities. The obligation relating to the legal representatives (Article 37) does not apply to data intermediation services providers and data altruism organisations.
Article 1.18, Article 32e.6 Data Act	Clarification added that registered entities shall notify the competent authority within a reasonable time about any subsequent changes to the information provided during the application process.
Article 1.18, Article 32i.2(c) Data Act	"Documents" can also be sensitive and therefore excluded from access, so added for consistency.
Article 1.18, Article 32i.3(b)(ii) Data Act	Linguistic modifications to facilitate the reading of the provision.
Article 1.18, Article 32i.3(d) Data Act	Clarification that industrial property rights are treated the same way as intellectual property rights.
Article 1.18, Article 32i.10 Data Act	Provides for the entry into application of Chapter VIIc only after a transition period of 18 months (previously contained in Article 11 of the Omnibus). This is a change of legal technique but not of substance.
Article 1.18, Article 32l.2 Data Act	The deletion reflects the existing practice.

Article 1.18, Article 32la.2 Data Act	The added sentence in the last part allows the authorities to extend the 20 days deadline to a total of 2 months in case of complex requests, and to a total of 3 months in case of protected data.
Article 1.18, Article 32p.2 Data Act	To address concerns that that the obligation will lead to a waste of resources even where not necessary.
Article 1.18, Article 32q.1 Data Act	The additions allow the competent authority to charge if searching and compiling the requested data is burdensome, and to remove information protected by law in addition to measures taken to protection commercially confidential information.
Article 1.18, Article 32w.2(b) and Article 32w.5 Data Act	The changes represent clarifications. "Documents" was added for consistency. Second, since point (b) refers to confidential data and documents, the reference to data subjects' consent under the GDPR did not make sense. Paragraph 5 is clarified as consequential change, since the provision does relate again to commercially confidential information and intellectual property rights.
Article 1.18, Article 33.1(d) Data Act	In paragraph 1 point (d) reference to smart contracts was deleted.
Article 1.18, Article 33(b) Data Act	Article 33(2) referred to Article 42 (c)(iii) which is deleted in this Omnibus
Article 1.18, Article 37(1)(b) Data Act	Deleting Paragraph 3 is important to make clear that the supervisory authorities referred to here, do not enforce the DA.
Article 1.20, Article 40 Data Act	Deleting paragraphs 4 and 5 is important to make clear that the supervisory authorities referred to here, do not enforce the DA. As editorial consequence, a new paragraph 4 is added, which had been introduced as paragraph 6 in the last drafting suggestion.
Article 10.1(2)-(4)	The last compromise text did not include the repeal provisions by clerical/IT error. The repeal period now is aligned with the introduced 18 months' transition period.
GDPR and ePrivacy	
Article 3(1)(a)	No changes compared to the previous compromise text.
Article 3(1)(b)	In line with the deletion of Article 8a (formerly Article 88b), definitions of notions used have been deleted. No changes compared to the previous compromise text regarding the definition of "scientific research".
Article 3(2)	No changes compared to the previous compromise text.
Article 3(3)(a)	Clarification with reference to the "technical operation" of an AI system or AI model. Addition of "strictly" to the derogation related to biometric verification.
Article 3(3)(b)	Amendments to include further clarifications and further details on the obligation of erasure of sensitive data ("without undue delay", "technically impossible").

	The last sentence has been moved to the corresponding recital to avoid interfering interpretation with the already existing accountability principle applicable to all GDPR provisions.
Article 3(4)	No changes compared to the previous compromise text. However, the compromise text includes a bracketed suggestion for alternative wording to be discussed during the meeting.
Article 3(5)	The proposed new Paragraph 5 has been restructured and simplified, derogating from Paragraphs 1 and 2 only, and to include a cumulative list of circumstances that must be met in order for the derogation to the information obligations to apply.
Article 3(6)	No changes compared to the previous compromise text.
Article 3(7)	No changes compared to the previous compromise text.
Article 3(7a)	Wording updates.
Article 3(8)	Amendments to revert the deadline for data breach notification to 96 hours. Wording updates in Paragraph 7 to ensure consistency between the update of the template and the adoption of an implementing act by the Commission.
Article 3(9)	Wording updates in Paragraph 7 to ensure consistency between the update of the template and the adoption of an implementing act by the Commission.
Article 3(9a)	No changes compared to the previous compromise text.
Article 3(10)	Updated version of Article 29a to be discussed during the meeting. Amendments to reduce the timeline for the EDPB to adopt its Opinion from 12 to 6 months.
Article 3(11)(ab)	No changes compared to the previous compromise text.
Article 3(12)	No changes compared to the previous compromise text.
Article 3(12a)	No changes compared to the previous compromise text.
Article 3(13)	No changes compared to the previous compromise text.
Article 3(14)	No changes compared to the previous compromise text.
Article 3(15)	Deletion of the proposed Article 88a, no changes compared to the previous compromise text. Deletion of proposed Article 88b and newly proposed Article 8a following Coreper guidance. Deletion of the proposed Article 88c, no changes compared to the previous compromise text.
Article 4	All amendments to Regulation 2018/1725 (EUDPR) have been aligned with the compromise text under Article 3. Further adjustments may be necessary for the complete alignment with terms and provisions of the EUDPR.
Article 5(1)	No changes compared to the previous compromise text.
Article 5(2)	Updated version of the amendment to Article 5(3) ePrivacy Directive, clarifying the whitelist of consent exemptions, including an additional exemption in relation to fraud prevention. Wording alignment with the ePrivacy Directive.
Article 5(2a)	No changes compared to the previous compromise text.
Cyber	

Article 6(1) – Art. 23a	The wording of the Article establishing the incident reporting information point has been further streamlined while preserving the main elements of information to be provided. Additional clarification has been added to refer to other group or bodies established at EU level. The reference to help guides and tutorials has been removed. Clerical mistake in Paragraph 2: second subparagraph should be numbered as "(b)" instead of "(c)".
Article 6(1a) – Art. 23b	The Article establishing the national entry point has been updated and restructured in order to further reflect the need for flexibility and consistency in the setting up of the entry point by Member States. – Paragraph 1 list the core tasks of a national entry point to be considered and allowed by Member States in setting up their national entry point ("at least one"). – Paragraph 2 provides for additional tasks that may be carried through the national entry point. – Paragraph 3 (formerly paragraph 2) maintains the original provision on Member States retaining flexibility to configure their national entry point, with a clarified reference to national structures. – Paragraph 4 (formerly paragraph 3) clarifies that Member States shall endeavour to design their national entry point with a view to achieve interoperability. – Paragraph 5 (formerly paragraph 4) adds clarification regarding the non-binding character of ENISA's recommendation. – A new paragraph 6 has been added, mandating ENISA, in cooperation with Member States, to develop an open-source solution that may be used by Member States in setting up their national entry point.
Article 6(1b) – Article 23c	The Article on harmonising incident notification framework has been updated with some wording adjustments and clarification, in particular under paragraph (1) with a reference to "further harmonisation" instead of "unified approach".
Article 6(1c) – Article 23d	The Article on cross border incident notification has been further streamlined and clarified through wording adjustment, in particular in paragraph (3), now simply stating that Member States shall retain control over the scope of information and any access to such information.
Article 6(2)	Wording update to refer to the incident reporting information point established under Article 23a.
Article 6(3)	No changes compared to the previous compromise text.
Article 7	No changes compared to the previous compromise text.
Article 8	No changes compared to the previous compromise text.
Article 9	No changes compared to the previous compromise text.
P2B	
Article 10	Article 18(1) is maintained in force, to ensure that the remaining articles of the P2B regulation are reviewed regularly, every 3 years.