Council of the European Union
General Secretariat

Interinstitutional files:
2025/0360 (COD)

Brussels, 15 December 2025

WK 17297/2025 INIT

LIMITE

SIMPL
ANTICI
DATAPROTECT
CYBER
TELECOM
CODEC
PROCIV
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 – Presentation by the Commission (AGS on 12 December)

Delegations will find enclosed a presentation as prepared by the Commission for the meeting of the Antici Group (Simplification) on 12 December regarding the Digital Omnibus (Omnibus VII).

1

Platform-to-Business Regulation

2

P2B

Which provisions are maintained?

The Commission proposes to maintain:

- The definitions of "**business user**" (Art 2.1), "**online intermediation service**" (Art 2.2) and "**online search engine**" (Art 2.5)
- Provisions on **restriction, suspension and termination** of an online intermediation service vis-à-vis the business user (Art 4)
- Obligation to put in place an **internal complaint-handling system** for online platforms (Art 11)
- **Enforcement** (Art 15)

3

P2B

How does the transition period work?

During the transition period, **until 31 December 2032**:

- The maintained definitions and provisions **remain in application** by virtue of the Digital Omnibus Regulation (no need for "re-entry" into force via P2B)
  - Example: the Platform Workers Directive will **continue to rely on the remaining P2B provisions** for the protections of self-employed platform workers;
- Those acts that contain cross-references to the P2B Regulation are to be **amended** in this time period.

4

P2B

What impact of the partial repeal of the P2B Regulation?

- Report on the interplay of the DSA with other legislation (the so-called "Article 91 report") was key in **assessing the added value of the P2B Regulation**: it concluded "several overlapping points" with the DSA (see here)
- Preliminary assessment of P2B (2023, here) concluded "lack of awareness", "insufficient compliance", "lack of implementation" and hardly any complaints had been received.
- **Impact on SMEs**: imbalances in trading relationships between business users and online platforms are addressed in DSA, with alleviations for micro and small enterprises. Stronger protections by corresponding DMA provisions which go beyond mere transparency.

→ **Clearer regulatory framework** avoiding overlapping and layered rules: **reduction of compliance costs**

5

P2B

How do the DSA and DMA cover the repealed P2B provisions?

• **Transparency of terms and conditions** of online platforms (Art 3 and 8 P2B)	• DSA provides for **transparency of terms and conditions** (Art 14 + 17 DSA), beyond direct contractual relationships
• **Self-preferencing**, such as in ranking results (Art 5 + 7 P2B): transparency in terms and conditions	• DSA provides for **algorithmic transparency** (Art 27) + risk assessment for Very Large Online Search Engines (Art 34.2) • DMA **prohibits self-preferencing** thereby going beyond transparency in P2B (Art 6.5 and 6.12)
• **Description on access to data**, if any, generated or used in the context of the service used by the business user (Art 9 P2B)	• DMA **goes further** and **obliges gatekeepers to allow access to such data** under certain conditions (Art 6.10 DMA)

6

P2B

What is the delta and what is the impact? (1/2)

- No requirement to provide information to business users on a «**durable medium**» (Art 3.2)
- No explicit prior notice for informing about **changes** in terms and conditions (Art 3.2)

→

- **Outdated** means of communication
- DSA obliges online platforms to inform business users of significant changes to the terms and conditions (Art 14.2)
- DSA obliges Very Large Online Platforms to publish a **summary** of their terms and conditions, have them **publicly available** in **all official EU languages**, and include available **remedies and redress** mechanisms (Art 14.5 and 14.6)

7

P2B

What is the delta and what is the impact? (2/2)

- **Micro- and small platforms** not in scope for some provisions of DSA
- **Smaller search engines** not covered by DSA provisions on ranking
- DMA doesn't cover smaller platforms

→

- Alleviation of **burden** and **focus on asymmetrical B2B relationships**
- DSA obliges Very Large Search Engines to risk assess their **algorithmic systems** (Art 34.2)
- DMA applies for search engines that are **gatekeepers**
- Focus on asymmetrical B2B relationships and **impact on fairness** of B2B relationship

8

P2B

What goals does the partial repeal seek to achieve?

- **Simplification** of the regulatory framework
- **Reducing compliance costs** due to overlapping and multi-layered rules
- Ensure **legal certainty** by providing for a transition period:
  - Example: P2B provisions which contain **deadlines** are maintained: online platforms continue to be subject to mandatory 30-day notice period when restricting, suspending or terminating services or accounts of business users (Art 4 P2B)
- More **robust and focused enforcement**
- Not a 1:1 identical coverage: minimal delta acceptable for the reasons above

9

Data

Data Act

10

Four to one

Data sharing of IoT data (personal and non-personal data from connected products & related services), rules on fair data-sharing clauses in B2B contracts, Business to Government data sharing, rules on cloud switching.

Data Act

Re-use of protected data held by public sector bodies increase data sharing (data intermediation services, data altruism), governance (EDIB).

Data Governance Act

Ensure the free flow of non-personal data within the Union (prohibition of data localization requirements), provisions on cloud.

Free Flow of Non-Personal Data Regulation

Re-use of public sector information, including research data and high value data sets.

Open Data Directive

11

11

Data Act – general questions on consolidation

12

Data Act

How does consolidating instruments incorporating other legal acts with different subject matters and scopes into the Data Act aid consistency and simplification of the legal acquis?

- The proposal integrates the data law acquis into a unified text and repeals DGA, FFNPD as well as ODD.
- This reduces the number of applicable regulations/directives *per se* and simplifies compliance – stakeholders will only need to consult a single document. In particular, the parallel regime of ODD and DGA is unified.

13

Data Act

Is the harmonisation of definitions not excluding sector-specific nuances that are necessary for regulated areas (e.g. health, fianance, telecommunications)?

- All changes were carefully assessed so this should not be the case.

14

Data Act

What is the relationship between the amended Data Act and the GDPR and how do the changes affect Art 1(5) Data Act (= non-prejudice and obligation to comply with Union and national law on data protection & privacy)?

- Amended Data Act does not change the relationship:
  - Data Act for both personal and non-personal data
  - GDPR obligations apply additionally for personal data.
- In case of conflict "[…] *with Union law on the protection of personal data or privacy, or national legislation adopted in accordance with such Union law, the relevant Union or national law on the protection of personal data or privacy shall prevail.*" (Art. 1 (5) last sentence excerpt Data Act).
- Consolidation do not change safeguards in place.
- Art 1(5) applies to all chapters – including newly added ones → all requirements in particular of the GDPR and the ePrivacy Directive must be met.
- No change in substance for former DGA, ODD chapters.
- Definitions are fully aligned (eg the more stringent definition of anonymization under the ODD was deleted).

15

Data Act

How does the consolidation of the instruments affect the structure for national competent authorities? If more than one are appointed, would a data coordinator be necessary?

- It is up to the Member States to decide whether the national competent authority under the current Data Act should also be responsible for the newly inserted chapters.
- It depends how global the attributions for the competences were made under national law. Eg if a national law specifies the chapter for which the authority shall be competent it would only be competent for those.
- For competent authorities under those acts that are being repealed it is up to the Member States to update their conferral of competence under national law.
- If you have more than one authority, a data coordinator is necessary.

16

Data Act

Does the right to complaint under Article 38 Data Act apply to all chapters of the consolidated Data Act?

- Special rules (means of redress) under the rules of the Open Data Directive and Chapter II DGA are maintained, as these regimes serve different purposes.
- For B2G:
  - No changes to right to issue a complaint
  - Merging of unnecessary duplications in Articles 17(5), 18(5), 20(5) and partially 21(5) into a simplified/unified complaints provision in Article 22a ('Right to lodge a complaint').

17

Data Act

What is the timeline for the data proposal?

- The aim is to have the Omnibus adopted as quickly as possible to bring immediate relief to businesses and citizens.
- In line with this objective, the COM proposes the Digital Omnibus to generally enter into application on the third day following that of its publication in the OJEU.

18

Data Act

What are the implications (and potential challenges, eg contradictions to national laws in place) arising from the fact that a Regulation is amending Directives?

- The proposed approach was carefully assessed. It is possible to change Directives with Regulations in specific cases. One of them being where a regulation replaces a directive as is the case with the Open Data Directive.
- On the Open Data Directive in particular:
  - In line with the principle of primacy of EU law, in case of contradictions between EU and national law, national authorities and courts must refuse to apply the national provisions.
  - It is for the Member States to ensure that their national law does not conflict or overlap with the Regulation.
- We do not foresee implementation or transposition challenges. To the contrary, the new rules will allow for a uniform approach within the EU and will prevent contradictory approaches among the different MS.

19

Data Act

How will consistency with other EU initiatives, eg the Data Union Strategy be achieved and why is there no definition of synthetic data in the Omnibus, if it is one of the focal points of the Strategy?

- The Data Union Strategy and the Digital Omnibus complement each other. Simplification does not come from regulatory simplification alone – other measures are necessary to ensures that true results are achieved. The Data Union Strategy sets out such additional non-regulatory measures and outlines further simplification ambitions.
- The Digital Omnibus Proposal does not specifically regulate synthetic data, thus it is not defined explicitly.

20

Data Labs

Which type of entity or entities (public/private) can launch a data lab?
Are data labs limited to Common European Data Spaces or can they offer their services to industrial/private-sector Data Spaces or to DIPS ?

- Data Labs will provide data-related services (curation, labelling, annotation, anonymization, etc.) to support public and private stakeholders who need access to high-quality data to develop and train innovative services, e.g., AI-driven services.
- Data Labs will act as practical interface between the AI ecosystem, common European data spaces, and data resources in general.
- The first Data Labs will be run in the upcoming AI factories – nothing prevents stakeholders from launching their own data lab according their needs.

21

Data Act

Will there be further integration of the Data Acquis in the Interoperable Europe Act?

- By default, the Commission assesses if/to what extent integration with other legislative initiatives and existing legal acts is needed.
- The Commission recognizes that issues with governance remain. Questions of how to clarify and simplify questions of governance should be addressed as part of the Digital Fitness Check.

22

Data Act

Why does the text not contain explict horizontal provisions on the availability of data within the framework of data spaces?

- The Digital Omnibus Proposal integrates the framework for Data Intermediation Services and Data Altruism Organisations from the DGA and the obligations for participants in Data Spaces from the Data Act taking into account that Data Intermediation Services and Data Altruism Organisations are not necessarily Data Spaces or vice versa.
- Given the scope of the Omnibus as simplification exercise, it seems not adequate to include new horizontal provisions, potentially increasing burdens.

23

Data Act

What is the evidence supporting the changes and the state of play of the studies?

- Documentation of Stakeholder consultations in Annex of Staff Working Document
- 2 studies were conducted:
  - Study supporting the evaluation of the Free Flow of Non-Personal Data Regulation, Open Data Directive and Data Governance Act (forthcoming – expected January 2026)
  - Study on the next data frontier that focuses on generative AI, regulatory compliance and international dimensions. Published on 1/12/2025 in EC library

24

Data Act

How will the impact of the newly added chapters in the Data Act be assessed – especially with regards to SMEs/SMCs?

- Included as part of review procedure (Article 49 Data Act).

25

Data Act

Can we delete or modify, as part of the Digital Simplification Omnibus Regulation Article 10(5) of the Data Act which obliges Member States to certify dispute settlement bodies?

- The Commission proposal does not include Article 10 of the Data Act.

26

Data Act – B2G

27

Data Act – B2G

Why does the EC deem that clarifications regarding trade secrets in relation to the public sector are necessary?

- The Omnibus does not change provisions in the B2G chapter of the Data Act on how trade secrets are to be handled and their confidentiality preserved.

28

Data Act – B2G

Why is there a focus on 'public emergencies', but the newly proposed Art 15a(1) still uses the term 'exceptional need'?

- A definition of 'exceptional need' is unnecessary, as the scope of Chapter V is wholly focused on 'public emergencies' and that term is well defined in Article 2(29).
- The use of the term 'exceptional need' in Article 15a(1) does not affect the operation of the Chapter.
- Deleting the uncertain "exceptional need" route in Article 15(1)(b)(ii), which allowed requests for data for non-emergency situations, simplifies the process, brings clarity and reduces burdens.

29

Data Act – B2G

How do you determine whether non-personal data are insufficient to respond to a public emergency?

- No material change by the Omnibus: overall mechanism is preserved, as well as 'public emergency' definition.
- The requesting EU or public sector body must, on a case-by-case basis, assess and demonstrate whether personal data are necessary to respond to public emergency, subject to appropriate safeguards.

30

Data Act – B2G

What is the rationale of Article 15a (2) vs. (3)?

- Art. 15a (1) → General duty for businesses to provide data to public bodies to respond, mitigate, or support the recovery from a public emergency.
- Art. 15a (2) → Applies when a public body requests data to respond to a public emergency. Personal data can be exceptionally requested. Enterprises of all sizes concerned.
- Art. 15a (3) → Applies when a public body requests data to mitigate or support the recovery from a public emergency. Personal data cannot be requested. Small and micro enterprises exempted.

31

Data Act – B2G

What is the added value of paragraph (3) in article 15a, given that it states it must be based on 'Union law or national law'?

- The wording in Article 15a(3) follows from the original Article 15(1)(b)(i).
- Same requirement for the requesting body to act on the basis of EU or national law.

32

Data Act – B2G

In Art. 21, 'the technical protection' currently appears in point (c) but should belong to point (d) together with the organizational protection measures. Is this a mistake?

- This is indeed an editorial mistake. Art. 21(5) point c) and d) should read:

"(c) the period for which the data is to be used;
(d) **the technical protection and** organisational measures taken, including where personal data or trade secrets are involved."

33

Data Act – Smart contracts

34

Data Act – smart contracts

What is the impact of deleting Article 36 on Article 35, and more specifically on Article 35(5)?

- The Omnibus proposal deletes Article 36, "Essential requirements regarding smart contracts for executing data sharing agreements".
- This has no impact on Article 35 or 35(5). Article 35 concerns "Interoperability of data processing services" and cloud interoperability standardisation.
- The substance and processes for Article 35 and 36 are separate.

35

Data Act – Cloud

36

Data Act – Cloud

How will the changes affect the market and how can the goal to remove the lock-in effect for users be maintained?

- Limited effects on the market – new contracts and services (after 12.09.2025) fully in scope.
- The exemption does not apply to the obligation to remove switching charges (Article 29 DA).

37

Data Act – Cloud

Does the exception also apply when the customization takes place via third party service providers that operate the changes?

- The exemption in Article 31(1a) only applies when the customisation is done by the provider of data processing services, if the provision of such services is based on a contract concluded before or on 12 September 2025.

38

Data Act – Cloud

What will the coordination mechanism be between national competent authorities responsible for the enforcement of the cloud switching rules?

•Under the current Article 35(6) of the Data Act, competent authorities will be systematically consulted on draft implementing acts.

39

Data Act – Cloud

Why is the exemption under Art. 31(1a) limited to services referred to in Article 30(1) and not those in Article 30(2)?

• Article 31(1a) should be read the other way around.
•The exemption foreseen in Article 31(1a) only applies to data processing services referred to in Article 30(2) (i.e. of the SaaS and PaaS types) as those are the ones that are generally customised and adapted to the needs of a specific customer.
•The exemption does not apply to data processing services referred to in Article 30(1) (those of the IaaS type).

40

Data Act – Cloud

Will the Commission provide guidance on the concept of 'custom-built' services to help providers and customers?

• At this stage, the Commission does not plan on issuing further guidance on this question.

41

Data Act – Cloud

How will the Commission assess the impact of the exemption in Article 31(1b) on SMEs and small mid-caps, especially regarding anticompetitive practices?

• As foreseen in Article 49(1) and (2), the Commission will carry out an evaluation of the Data Act, including on the cloud switching rules with a special focus on SME providers.

42

Data Act – Cloud

In case of side effects following the exemption in Article 31(1b), does the Commission foresees revision mechanism to ensure the achievement of the objectives of the Data Act?

• Article 31(1b) introduces an exemption for providers of data processing services that are SMEs and small mid-caps only for contracts concluded before the entry into force of the Data Act.
•Contracts for the provision of data processing services concluded after 12 September 2025 will not be covered by this exemption and will need to fully comply with all the cloud switching rules even when provided by SMEs/ small mid-caps.
•This narrow exemption will not jeopardise the objectives of the Data Act.

43

Data Act – Cloud

How will the Commission ensure that the exemption provided to SMEs and small mid-caps under Art. 31(1b) will not lead to a reduction in the level of protection for consumers?

• The clarification and exemption under Article 31(1b) only cover contracts concluded before the Data Act entered into force (12 September 2025).
•The parties will continue to be bound by the contractual terms they agreed to until the contract ends or is terminated by one of the parties.
•Therefore, this exemption will not lead to a reduction of the level of protection for customers.

44

Data Act – Cloud

Do the cloud switching obligations that apply to SaaS only cover data processing services provided by cloud or edge providers or do they apply to any SaaS software provider?

- The obligations of the Data Act apply to all services which display the characteristics listed in the definition of 'data processing services' in Article 2(8).
- The fact that a software is built in and provided via a cloud environment, makes itself use of data processing services, or processes the data collected from the usage of the software is not in and of itself sufficient for that software to qualify as a data processing service under Article 2(8). It is not sufficient that a service merely makes use of the resources referred to in Article 2(8) for the provision of another service to be considered as a 'data processing service'.

45

Data Act – International Data Transfers

46

Data Act – International Data Transfers

Are there inconsistencies between provisions related to international data transfers in GDPR, Data Act and Data Governance act, given the different formulations?

- There is a fundamental difference between the provisions of chapter V GDPR which indeed governs transfers of personal data to non-EU countries and Article 31 DGA and 32 Data Act.
- The latter two only regulate obligations of entities receiving non-personal data access requests from foreign governmental entities.
- Article 31 DGA and 32 Data Act - the provision that will be kept after the insertions -, on the other hand, are virtually identical.

47

Data Act – International Data Transfers

What is the rationale to merge Article 31 (1) and (2) of the Data Governance Act and Article 32 (1) and (2) of the Data Act?

- The Omnibus merges Article 31(1) and (2) of the Data Governance Act with Article 32 (1) and (2) of the Data Act because the provisions were virtually identical except for the entities they regulated.
- The Omnibus is clearer because it lists, in a simplified rule, the regulated entities.

48

Data Act – International Data Transfers

Can you clarify the requirements of proposed Article 32, which concerns non-personal data, and Article 32w (ex Art. 5 DGA), which concerns both personal and non-personal data? What kind of technical, legal or organizational measures do you envision as being adequate in the context of sharing protected non-personal data?

- Both Article 31 DGA (elements in Article 32 Data Act) and Article 5(9)-(14) (Article 32x) DGA concerned non-personal data. That has been maintained in the relevant articles.
- The necessary technical, legal and organizational measures will depend on the case.

49

Data Act – International Data Transfers

What is the interaction between Article 32 Data Act (unlawful international governmental access and transfer of non-personal data) and NIS2 Directive?

- The Data Act mandates "adequate measures" to prevent unlawful access and transfer of non-personal data held in the EU by third country governments.
- NIS2 requires organizations to implement risk management, incident reporting and cybersecurity measures.
- Entities under both regimes must protect against system breaches and unlawful third country government access.

50

Data Act – International Data Transfers

Does the COM envisage establishing a cooperation mechanism and a technical instrument for cooperation between competent authorities as regards international data transfers?

- No, this is currently not foreseen. However, such discussions may take place in the context of EDIB.

51

Data Act – Free Flow of Non-personal Data Regulation

52

Data Act – Free Flow of Non-personal Data Regulation

How will the Commission ensure the uniform application of the prohibition on data localisation requirements and the necessary transparency regarding national exceptions?

- The prohibition on unjustified data localisation requirements from the FFDR remains in place in the form of Art. 32h.
- Member states are obliged to immediately communicate relevant draft acts to the COM (Art. 32h (2)).

53

Data Act – Free Flow of Non-personal Data Regulation

How would the deletion of the national contact point be organized concretely?

- The obligation to notify the Commission of localisation requirements would be maintained.
- The proposal abolishes the national online single information point where Member States should publish applicable data localisation requirements.

54

Data Act – Free Flow of Non-personal Data Regulation

Is sensitive data, access to which could pose a threat to public security, public order, health or intellectual property, out of scope?

- The original FFoD (and Art 32(h) Omnibus) only **prohibits unjustified intra-EU** data localization requirements **for non-personal data**.
- As an exception to the rule, Member State may impose data localization requirements vis-à-vis another Member State if the data localization restriction is **justified on grounds of public security and in compliance with the principle of proportionality**. Moreover, Union law may also impose data localization requirements within the Union, in line with the Union's international commitments.

55

Data Act – Free Flow of Non-personal Data Regulation

Would a general policy or a specific provision in certain procurement procedures requiring the processing of data and/or the localisation of servers <u>within the EU</u> fall under the proposed Art. 32(h)?

- A Member State imposing an intra-EU data localization requirement vis-à-vis one or more third countries is not covered by Article 32(h).
- Such a provision would have to be in line with international commitments taken by the EU and Member State.

56

Data Act – Free Flow of Non-personal Data Regulation

What if secure processing environments under Article 32w may, in practice, necessitate nationally hosted or otherwise domestically controlled infrastructure? Would that be counter to the prohibition of data localisation?

- The prohibition of data localization requirements is not in contradiction with an obligation imposed by a public sector body to process data that that public sector body holds in the IT systems of that public sector body.
- This is not about the localization of the processing, but about the public sector body being able to verify the compliance of the processing operations with the conditions imposed under Article 32w (and currently Article 5 DGA).
- In any event, the secure processing environment may be itself a cloud-based system, the hosting of which in a specific MS is not mandated by this provision.

57

Data Act – EDIB

58

Data Act - EDIB

How will the changes to EDIB affect the functioning and efficiency of meetings?

- Outcome: Commission will be able to manage participation better → "shall decide on the composition of the different configurations" (Art 41a(3))
- Intention: separate enforcement questions from strategic discussion (now involving competent MS ministries)
- However: EDIB will not have mandate beyond consultation (no role in comitology, no essential role in legislative process)

59

Data Act - EDIB

Will the EDIB coordinate with other boards (e.g. AI Board, EDPB, Interoperable Europa Board)?

- The Commission will increase its efforts to coordinate these boards better internally.

60

Data Act - EDIB

Will the EDIB have competences for Chapters VI, VIII, VIIc?

- The EDIB was not competent for questions of implementation of Chapter VI and VIII under the Data Act (cloud switching and related standardization).
- The coordination among competent authorities for the cloud switching provisions of the Data Act will be clarified in the upcoming Digital Networks Act (DNA). The DNA will review the tasks of BEREC and the Commission is considering to use this opportunity to clarify that BEREC is responsible for facilitating regular exchanges among national competent authorities responsible for the application and enforcement of Articles 23 to 31 and Articles 34 and 35 of the Data Act.
- EDIB should, however, have competence for chapter VIIc (re-use of public sector information). Tasks previously were taken up by a separate Commission expert group, the Public Sector Information Group, which is intended to be merged with the EDIB.

61

Data Act – Data Intermediation Services Providers (DISPs) & Data Altruism Organisations (DAOs)

62

Data Act – DISPs & DAOs

How can the voluntary registration incentivize the uptake on the market?

- Mandatory DISP regime perceived as "straitjacket"
- New DISP regime:
  - Possible to offer services without strict requirements needed for registration and label
  - Label can be used to reap benefits/increase trust
  - No functional separation needed for DISPS that are micro/small enterprises to register
- DAOs: Burden reduction as reporting obligations disappear (DAOs are free to report on their activities and may have to as a result of national law on not-for-profit organisations).
- Use of label still can lead to reputational advantage and generating trust.

63

Data Act – DISPs & DAOs

Does the COM consider rolling out a technical system to report the registry entries to the COM?

- Given the current low number of registrations, this has not been deemed necessary.
- We do not expect this number to become unmanageable in the future, especially with the now voluntary registration for data intermediation services providers.

64

Data Act – Re-use regime: Merging ODD and Chapter II DGA

65

Data Act – Re-use regime

What is the interplay between the different sections of the new chapter VIIc on re-use of public sector information?

- Section 1: Scope of application and common principles (data and documents)
- Section 2: ODD (data and documents)
- Section 3: Chapter II DGA (data and documents)

Overview of Article 32i on Scope:

- Article 32i(1)&(2): scope of application that accommodates ODD and Chapter II DGA rules
- Article 32i(3): ODD Scope of application
- Section 32i(4): Chapter II DGA scope of application

66

Data Act – Re-use regime

How will the new Act ensure the continued enforcement of the fundamental principles of accessibility to open public-sector data, which are separate from and different to the frameworks for the re-use of chargeable data addressed by the Data Act and the Data Governance Act?

- The integration into the Data Act as well as the merging of common provisions does not change the principle of open data.
- The regimes were kept separate where necessary to ensure that progress made for the availability of open sector data is not lost.
- The proposed amendments merely integrate the provisions into a new instrument. The scope for Open Data remains the same.

67

Data Act – Re-use regime

Which personal data is in scope of VIIc Section 2?

- The same personal data that was in scope of ODD.

68

Data Act – Re-use regime

Is protected data held by public undertakings now in scope?

- Identical to the current situation: data and documents held by (certain) public undertakings are in scope of VIIc Section 2 (ex ODD) but not in scope of VIIc Section 3 (ex Ch II DGA).

69

Data Act – Re-use regime

Can you explain the definition of data and documents and what is digitised/non-digitised?

ODD: before
Document covers everything:
- Any content* or its parts
- in digitised **and** non-digitised form

Data: **Digitised** document

DGA: before
Data: **Digital** content*
~~Documents~~

Data Act: after
Document:
- Any **non-digital** content* or its parts

Data:
- **Digital** content*

--> Chapter VII, VIIc relate to (non-digital) documents and (digital) data.

*Including sound, visual, audiovisual

70

Data Act – Re-use regime

Are non-digitised data or non-digitised documents now in scope?

- Before they were in scope of the ODD but not Ch II DGA. Now they are in scope of the ODD and Ch II DGA.
- No additional burden as public sector bodies do not need to share any data under Chapter II DGA (now Section 3 of Chapter VIIc).

71

Data Act – Re-use regime

Has the definition of re-use changed?

- The definition of re-use under the DGA was not extended.
- MS continue to be able to set specific conditions for reuse of protected data (32w, Art 5 DGA before). In principle, joint re-use by a number of third parties should be possible.

72

Data Act – Re-use regime

What is a public sector body and are there any changes for national central banks?

- Nothing changes with regard to the definition of public sector bodies according to DGA.
- Typical public sector bodies mandated to grant access to data are e.g. national statistical offices.
- Central banks remain in scope of "public sector bodies".
  - Member States do not need to modify or replace their existing dissemination frameworks that comply with ESCB statistical rules.
  - Member States do not need to exclude national central banks explicitly: The mere absence of a "competence under national law to grant or refuse access" (cf. 32w(1)) is sufficient to exempt central banks data from the obligation to grant access for re-use
  - Confidential datasets held by central banks do not need to be included in the national single information point or asset list unless already publicly available.

73

Data Act – Re-use regime

Are MS obliged to make data available?

- There **was and is no obligation** to make data available under ODD or Ch II DGA unless it is a High Value Dataset.

74

Data Act – Re-use regime

What exactly is achieved by integrating ODD and Chapter II DGA into the Data Act?

- Omnibus moves two regimes into one legal act and transforms ODD into regulation.
  - No national ODD transposition or interpretation of it --> fosters EU-wide data markets, data availability for society, indirect positive effect on public sector data flows.
  - No contradiction to national legislation transposing ODD as regulation takes precedence.
- Ch II DGA and ODD scope and obligations **remain the same**. However inter alia:
  - Ch II DGA now: includes non-digitised content, has info on means of redress & possibility for online payment
  - Art 5 DGA restructured, streamlined and moved into 32w, 32x without material changes
  - Ch II DGA and ODD now with possibility to have special conditions for "Very Large Enterprises"
  - Clarification on which regime is applicable where data has been anonymized.
- High value data sets are adopted with **delegated** instead of implementing act.

75

Data Act – Re-use regime

How is confidentiality/privacy preserved? How is sensitive data protected?

- Public sector bodies may establish certain requirements to protect data/documents (e.g. anonymisation, aggregation, secure processing environments).

76

Data Act – Re-use regime

Do MS remain free to go beyond the minimum harmonisation requirements of the ODD?

- Yes, Member States may go beyond. The minimum harmonisation principle of the Open Data Directive is maintained in the Data Act (see Article 1(13)).
- Therefore, national legislation on the ODD can continued to be used as far as compatible with this principle and the other rules of the proposed Data Act.

77

Data Act – Re-use regime

What is the interplay between the rules of the amended Data Act and the EHDS Regulation? Should this be clarified in the amended Regulation? Should an explicit reference to the EHDS be added? Is the EHDS secondary use fee structure changed?

- For a range of elements, the DGA is a common legal baseline. For certain elements, specified in the EDHS Regulation, the EHDS Regulation provides for more specific rules.
- The key difference between Ch II DGA and the EDHS Regulation is that the DGA does not lay down a right to secondary use of (any) protected public sector data.
- Our preference is to avoid – inevitably selective – references to sector-specific regulation. The EHDS Regulation contains a range of recitals and enacting terms that clarify the relationship with the Data Governance Act and the Data Act. These references remain valid also after the modifications brought by the Digital Omnibus.
- Article 62(2) third sentence EHDS Regulation clarifies that the charging rule in Article 6 of the DGA does not apply to public sector bodies in the EHDS secondary use context. There are no changes to this.

78

Data Act – Re-Use regime

Do the rules foreseen in the proposal alter the possibility to combine 'secure processing environments' under different data space regulations with the 'AI Regulatory sandboxes'?

- If this was possible before, the consolidated framework should not affect such an initiative.

79

Data Act – Re-use regime

Implementation, enforcement

80

Data Act – Re-use regime

Will MS have to change their ODD & DGA implementation structures?
Will this create unclear roles/obligations or require more resources?

- The structures set in place in order to comply with the ODD & DGA (competent bodies, single information point, competent authorities) can stay. Their tasks change only to a certain extent (voluntary regime for DISPs instead of compulsory → burden reduction for public bodies).
- The DGA single information point is transferred to 32aa without significant changes including the DGA requirement on necessary resources. The FFPD single information point is abolished.
- The Ex-Data Act and Ch III, IV enforcement structure in Article 37 is not competent for Ch VIIc (Ch II DGA or ODD).

81

Data Act – Re-use regime

What is the rationale of the amendments to the single information point (Chapter II DGA)?

- Deleted "may" provision to link the information point to sectoral, regional or local information points.
- Simplification & streamlining

82

Data Act – Re-Use regime

Could the Articles on single information points and open data publishing not be joined and synchronised?

- The proposal aimed at joining and synchronising Articles that were virtually the same (or very similar), bearing in mind not to cause too much burdens on Member States for the implementation.
- This is why the two regimes were kept separately.

83

Data Act – Re-use regime

High value data sets

84

Data Act – Re-use regime

Will the changes affect the implementing act on high value data sets? Is only open data in scope ? Will access be simplified for enterprises other than startups and SMEs?

- Empowerment to adopt act on high value data sets reproduced in proposal, now delegated act, no further substantive changes.
- Implementing act will remain in force and can be updated.
- List of high value data sets is a list of open data first established under the Open Data Directive. It generally concerns data held by public sector bodies and public undertakings.
- Under the current Open Data Directive, there are no specific privileges for startups or SMEs. Such privileges, for startups, SMEs or other enterprises do not seem warranted as data is, in principle, published pro-actively at no cost (exceptions for data held by public undertakings and certain cultural institutions).

85

Data Act – Re-use regime

In the context of High value data sets, what does "substantial part of their costs relating to the performance of their public tasks" mean? Is there a definition?

- As already under the Open Data Directive, there is no legal definition of that term.
- The provision has been integrated into the proposal without changes. The meaning stays the same.

86

Data Act – Re-use regime

Fees & Charging

87

Data Act – Re-use regime

In the context of Article 32y(2) (Fees in the context of re-use of protected data)

- **what does the reference to the State Aid rules mean?**
- **is it possible to apply lower fees to other kinds of entities than those mentions (SMEs, SMCs, civil society, research and educational establishments)?**

- This means the State aid rules laid down in Articles 107 – 109 TFEU. This is not new in principle. Recital 51 ODD says that the rules are without prejudice to the application of state aid rules: a Member State must check ex ante whether State aid may be involved in the relevant contractual arrangement and ensure that it complies with the State aid rules.
- It is possible to apply lower fees to other entities, as indicated by "in particular", the list of entities eligible s illustrative and non-exhaustive.

88

Data Act – Re-use regime

How would one implement the special conditions for very large enterprises and online platforms where data are open and freely available? How would one identify a very large enterprise where re-use is enabled without user identification?

- The idea is that public sector bodies may set out such special provisions where they know that such entities are re-using the data in question. This is an expansion of the possibility already in place under the Open Data Directive to set out conditions for the re-use (Article 11 ODD).
- Where it is not possible for a public sector body to identify the user, it will not be possible to set out special conditions.

89

Data Act – Re-Use regime

Will there be guidance on the fees and potential exemptions for e.g. Very Large Enterprises or SMEs?
Why are the fees from ODD and DGA not consolidated?

- MS are free to establish a fee catalogue in line with the regulation including possible exemptions e.g. for SMEs or Very Large Enterprises.
- ODD and DGA have different scopes/obligations: a unified fee structure would contravene the systematic and would put at risk progress made with the ODD.
- State aid rules (inter alia 107-109 TFEU) continue to apply.
- EDIB can look into this but no formal guidance is planned.

90

Data Act – Re-Use regime

Will the Commission issue any guidelines, e.g. on fees, Single Information Points, harmonised application of rules or secure processing environments?

- Currently not foreseen except:
  - DCAT-AP as common medata format for data.europa.eu (already in place)
  - EHDS technical specifications for secure processing environments shall be presented to MS once available.

91

Data

GDPR

92

Questions on Article 88a

93

Cookie rules

What are the implications of bringing parts of the cookie Article of the ePrivacy Directive under the GDPR?

- Access to the connected device of a natural person often constitutes or leads to the processing of personal data. Those cases should be brought under the strong protection framework of the GDPR
  - → Same regime
  - → Directly applicable (Directive to Regulation)
  - → More harmonization
  - → DPA enforcement
  - → GDPR fines: Many elements of the new articles rely on other GDPR provisions, that are subject to fines pursuant Article 83, e.g. lawfulness of processing, conditions of consent. Where the new articles provide for new elements, we will reflect.
- Article 5(3) of the ePrivacy Directive is maintained for connected devices of legal persons and non-personal data. This ensures that protection standards are not lowered.
- Protection of confidentiality is maintained in the ePrivacy Directive. The protection of personal data under the GDPR does not preclude that the personal data may be subject to other confidentiality rules, such as for instance the confidentiality of electronic communications or the medical secrecy.
- Relationship between GDPR and ePrivacy Directive will not change: Article 95 GDPR remains applicable – the carved out situation is however fully and entirely regulated by the GDPR.

94

Cookie rules

What is the impact on number of consent requests where the rules remain the same for non-personal data? What percentage of websites will display cookie banners again due to the exception in Article 88b(3)?

- Since the rules for non-personal data are not changed, no change for the number of consent requests is foreseen.
- The working assumptions for the calculation of savings were that 50% of private sector websites and 80% of public sector websites would no longer rely on consent and use cookie banners (cf. Staff Working Document SWD(2025) 836 accompanying the proposal, p50).
- It is difficult to estimate how many more cookie banners will be displayed because of the media exemption from central cookie settings, since media providers still could opt in to accepting centrally set cookie consent preferences.

95

Cookie rules

What is the scope of the carve out – when does Article 88a apply?

- Scope of Article 5(3) ePD carve out: 2 cumulative criteria
  - i) User or subscriber* is a natural person
  - ii) Information stored or access to the terminal equipment constitutes or leads to processing of personal data (not only for cookies)

→ If fulfilled: Article 88a GDPR applies
→ Otherwise: Article 5(3) ePD applies

- Scenarios received by Member States:
  - Subscriber and the user is a legal person, but the information stored or access leads to the processing of personal data: Article 5(3) for access, GDPR for processing
  - Non-personal data is stored on the terminal equipment and the subsequent processing leads to the processing of personal data: Art 88a applies.
  - The same access leads to or constitutes both processing of personal and non-personal data: Art 88a applies.
  - Controller cannot identify the natural person: Article 5(3). If the natural person is identifiable by using reasonable means Article 88a applies.

* Under the definition of Directive 97/66/EG subscriber can be a natural or a legal person.

96

Cookie rules

Does Art 5(3) apply where a processor does not have the means to identify a natural person?

- A "processor" as defined under the GDPR processes personal data for a controller. The controller defines if it needs to process personal data to achieve the set purpose.
- Where an entity only needs to collect non-personal data, Art 5(3) for the access to terminal equipment applies.

97

Cookie rules

What are the consequences of the proposed amendments to the notion of personal data for the cookie rules ?

- The proposed amendments to Art 4(1) GDPR do not change our understanding on what is personal data, but builds on recital 26 and case-law.
- 88a applies where the access constitutes or leads to the processing of personal data
- Example: Where a controller stores or gains access to information that is non-personal from the controller's point of view but can lead to the processing of personal data by a subsequent entity and the other entity would be subject to the GDPR.

98

Cookie rules

What does the exception from the consent requirement under Article 88a(2) mean?

- The provision mirrors Article 15(1) ePrivacy Directive – with explicit reference to the objectives of Article 23 GDPR.
- Member States may adopt national laws within the meaning of Article 6, for the objectives of Article 23 GDPR.
- For Article 5(3) ePrivacy Directive Article 15(1) continues to apply. 88a(2) cannot be used to introduce exceptions to Article 5(1) of the ePrivacy Directive.

99

Cookie rules

What is the relationship between the rules of the newly inserted Article 88a and 88b and the GDPR – in particular Article 6, including for rules on consent?

- GDPR applies fully: all principles and rules – including for consent apply.
- Whitelist: grounds for processing without consent for low-risk purposes directly provided for by the GDPR.
  - Also covers subsequent processing for the purposes listed.
    - = Subsequent processing addresses the processing after the storage or gaining access as mentioned in the first sentence of Article 88a(1).
    - ≠ "further compatible processing" in the sense of Article 6(4)
  - No additional legal basis under Art 6 required – eg no balancing test necessary.

100

Cookie rules

What are the new elements when it comes to the whitelist in Article 88a(3)?

- The exceptions to the consent requirement contain four grounds for which the subsequent processing will also be considered lawful.
- Current exemptions of Article 5(3) ePD last sentence are mirrored:
  - 88a(3)a: carrying out the transmission of an electronic communication over an electronic communications network
  - 88(3)b: providing a service explicitly requested by the data subject
- Two new exemptions for low-risk purposes:
  - 88a(3)(c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use
  - 88a(3)(d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service.
- Exemptions do not apply where Article 5(3) applies.

101

Cookie rules

What does the newly added whitelisted ground "aggregated information about the usage of an online service to measure the audience" mean (Article 88a(3)(c)) and how can abuse be prevented?

- Reflects idea that a provider of a website may want to understand how many people visit its website at specific times – just like the owner of a shop would like to understand when people visit his/her shop.
- ≠ official statistical data.
- Aggregation can be at the level of certain demographic indicators or geographical areas of use.
- Exemption only applies where aggregated information are used to measure the audience. This would exclude broader behavioural analytics for individuals by definition. Where such broader analytics are performed on aggregated information, the Commission would in principle not see greater risks for the rights on individuals.
- Narrow wording (≠ Audience Measurement in European Media Freedom Act) to limit scope. Editorial responsibility is required.
- General GDPR principles apply and protect against abuse – subject to GDPR enforcement and fine structure.

102

Cookie rules

88a(4): What is the relationship between the new rules (single click, 6 months limit, central cookie management) and the rules on consent under Article 7 GDPR?

- Article 88a(1): consent in accordance with GDPR – includes Art 7 GDPR
- Proposal does not amend GDPR principle and all other requirements.

→ Right to withdraw (Art 7(3))fully applies – no changes to the status quo.
→ Consent must be separated from acceptance of other terms and conditions (Art 7(2))
→ Proposal/GDPR do not take a position on validity of certain models.
→ No excessive cost for businesses – measures proportionate.

103

Cookie rules

88a(4): What does the reference to subsequent processing mean for the single click requirement and the 6 months limit?

- Subsequent processing addresses the processing after the storage or gaining access as mentioned in the first sentence of Article 88a(1) ≠ "further compatible processing" in the sense of Article 6(4).
- For 88a(4), this means that the rules stipulated in that paragraph also apply to consent where consent constitutes the legal basis for the subsequent processing of personal data.
- In other words: A controller is also bound to wait six months before asking for renewed consent for the data processing, following access to the device.
- It is important to note that the GDPR's principles and all other requirements continue to apply fully, this includes the compatibility test of Article 6(4) GDPR.

104

Cookie rules

Will the new rules impact default settings of connected devices ("terminal equipment")?

- Proposal does not touch upon default status.
- Where consent is required: principles of GDPR apply fully
- Article 7 GDPR: informed and specific

→ General rule continues to apply: where consent is necessary it needs to be asked and fulfill the requirements of Art 7

105

Questions on Article 88b – central cookie management

106

Cookie rules

What is the relationship between the requirements for consent (single click, 6 months) as outlined in 88a(4) and the provisions on central cookie management in 88b?

- **Art 88b = answer to reduce number of cookie banners via central settings:** sets out rules where data subjects set their preferences (in browser, in specific apps)
- **Art 88a(4)** = answer to tackle consent fatigue **where no central choice has been made** by the data subject.

- **Do the requirements of Article 88a(4) apply where preferences were set centrally?**
  - 6 month obligation continues to apply.
  - Single click applies but banner is not visible to that user.

107

Cookie rules

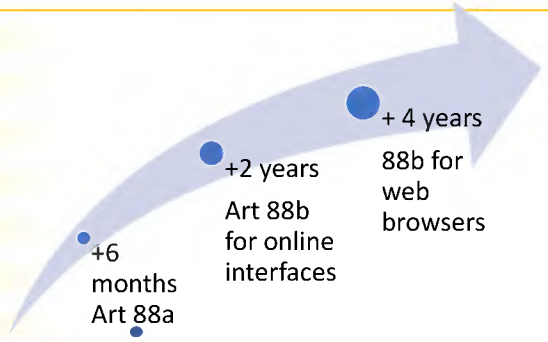
What do the exemptions under Article 88b relate to?

- **Media exemption**
  - The exemption in 88b is not an exemption from asking for consent. It is an exemption from the obligation to respect a signal indicating consent preferences of a user.
  - It only applies to Article 88b – still subject to measures in 88a(4) where media providers rely on consent.
  - There is no impact on the processing for journalistic purposes (Art 85(2) GDPR).
- **SME browser exemption** only applies to Article 88b.

108

Cookie rules

What are the timelines and how will a smooth transition be ensured for the new rules on cookies?



Entry into force:
3 days after publication in the Official Journal

Reason for different timelines of Art 88b:
The two-tiered approach should foster a volunteer, market-driven approach to the development and use of third-party browser plug-ins.

109

Other changes to ePrivacy Directive

Why was Article 4 ePD (security of electronic communications services) deleted?

- Has become obsolete in light of
  - Art 21 and 23 NIS2 Directive (provisions on cybersecurity risk-management measures, reporting obligations).

  and
  - Art 32-34 GDPR (provisions on security of processing, data breach notifications).

110

GDPR – Implementing acts on pseudonymisation techniques

Are implementing acts the right modus operandi to undertake such an assessment and does this not lead to interpretative authority of the notion of personal data by the Commission?

- **Aim**: Reduce legal uncertainty for companies that often struggle to understand when data resulting from pseudonymisation can be considered non-personal data for a receiving entity.
- **Why implementing act:**
  - CJEU jurisprudence is casuistic and develops gradually. The Court remains the ultimate authority for interpreting EU law.
  - Can be used by controllers to demonstrate that data is out of scope of GDPR – responsibility remains.
- **Scope:** specify the means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data
  - Assessment of techniques against the requirements of the GDPR and its interpretation by the courts and the data protection authorities.
  - Provide further clarity how controllers need to assess the risk of re-identification.
- **Fully respects powers of DPAs and the courts**: no intention to re-define what data are personal and what are not.
- The EDPB will be closely involved in this work process.

111

GDPR: Definition of personal data

- The proposed definition does not change the notion of personal data. It aims to address issues which are raised under the current wording.
- It builds on recital 26 GDPR and the standing case-law of the CJEU (Breyer, OC v European Commission, SRB).
- It brings legal certainty by codifying this standard in the operative part of the GDPR and contributes to a uniform application which is currently not the case.
- The GDPR applies to all entities who have "the means" reasonable likely to be used to identify the individual, even if they receive the data from an entity for which the data is not personal.
- The test of not having the "means" is very high: the risk of identification must be "non-existent or insignificant" (Breyer §46).
- Whether singling out an individual is so granular that it entails the processing of personal data is not affected by the proposed clarification.

112

GDPR: Definition of personal data 2

- On the impact of the change on international transfers: Chapter V GDPR is based on the premiss that the sender (controller in the EU) is responsible for GDPR compliance. If the sender has the "means reasonably likely", the data is personal for that sender, who thus must comply with Chapter V.
- On the impact on controller–processor relationship (Art 28 GDPR): since the processor processes the data on behalf of the controller (they undertake the processing activity jointly), no change. The SRB judgment did not elaborate on a controller-processor relationship, because that was not part of the facts of the contested decision. Therefore, the codification of the definition in the omnibus does not touch upon this point.

113

GDPR: Definition of personal data 3

- The CJEU and recital 26 GDPR already stated that data should not be considered personal data when the entity does not have the "means reasonably likely" to identify the natural person.
- On the meaning of "means reasonably likely to be used": this wording is the one of current recital 26 GDPR and was used by the CJEU in e.g. Breyer, OC v European Commission or SRB. DPAs are to provide for the interpretation of this notion on a case-by-case basis taking into account the factors mentioned in recital 26 GDPR.
- The proposed definition does not impact the fact that the "information enabling identification" must not be in the hands of the same entity. As long as a recipient has lawfully and realistically (SRB §82, Breyer §46) access to such additional information, the data is personal for this entity.

114

GDPR: Personal data processing for scientific research

- The proposed amendments address the lack of clarity about the conditions for scientific research:
  - Legally binding definition of scientific research;
  - Clarification of the conditions for compatible further processing;
  - Clarification that legitimate interest can be a basis for scientific research;
  - Extension of the exceptions from the information obligation for processing in case of scientific research under certain circumstances.
- They will facilitate the use of personal data to achieve research goals.
- Conditions and safeguards of Article 89 GDPR remain unchanged.
- All the other applicable GDPR rules and principles have to be respected.

115

GDPR: Personal data processing for scientific research 2

- The proposed definition of scientific research builds on recital 159 GDPR, Art 179 TFEU and the notion of 'ethical standards' (recital 33 GDPR).
- The terms of 'innovation' and 'actions' stem from Horizon Europe, the EU's key funding programme for research and innovation.
- Ethical standards, such as the principles of reliability, honesty, respect and accountability are stated in the ALLEA Code for research integrity.

[ALLEA is the European Federation of Academies of Sciences and Humanities. It brings together 59 Academies in more than 40 countries from the Council of Europe region.]

- Other examples of ethical standards established for medical research include: World Medical Association (WMA) Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Participants.

116

GDPR: Personal data processing for scientific research 3

- The amendment clarifies that a controller can further process the data it has already, for scientific research purposes. This clarification is needed since, although it was the wish of the legislator expressed in the GDPR, it has not always been interpreted accordingly. This hampers cross border research in the EU.
- Consequently, the controller can rely on the initial legal basis when further processing for scientific research purposes.
- It clarifies that scientific research constitutes a legitimate interest. The GDPR balances the right to protection of personal data, pursuant to Art 8 of the Charter of Fundamental Rights, with the freedom of science, pursuant to Art 13 of the Charter, as stated in recital 32 GDPR.
- However, the controller must ensure that all other conditions of Art 6(1)(f) (legitimate interest) and all other requirements and principles of the GDPR are met.
- Public sector can rely on Art 6(1)(e) for scientific research - no changes.

117

GDPR: Processing in the context of AI

What is the aim of Article 88c and how does it interplay with Article 6 GDPR and other sectoral laws?

- Article 88c is placed in the Chapter IX GDPR on specific processing situations, i.e. processing of personal data in the context of AI development & operation.
- Article 88c responds to the importance of AI for EU economic growth and its societal beneficial usages and aims at reassuring that the legal basis of Article 6.1.f GDPR may be relied upon, provided all conditions of Article 6.1.f as well as all other GDPR requirements are met.
- "Where appropriate" precisely indicates that it is up to the controller –according to the current regime- to choose the appropriate lawful ground of processing pursuant to Article 6 GDPR. Article 88c does not affect this obligation nor overrules other sectoral laws requiring, for example, consent, setting out a legal obligation or providing for the processing for an objective of public interest, in compliance with Article 6(1)(c) or Article 6(1)(e) and Article 6(3) GDPR.
- Article 88c(2) does not affect conditions set out in other Union law, such as Article 71 Reg 2025/327 (EHDS) on the unconditional right to object and its limitations in the context of secondary use of health data.
- Similarly, Article 88c does not affect laws setting out prohibitions, such as Article 5 AI Act.
- Recital (30) explains the obligation of the controller to ensure compliance with other Union or national laws.

118

GDPR: Processing in the context of AI

How is it ensured that AI development and operation do not constitute legitimate interests and which legitimate interests could be pursued under Article 88c?

- The wording of Article 88c states "for the interests of the controller in the context of AI development and operation", which means that AI development and operation do not in themselves constitute legitimate interests.
- For instance, improving accessibility of a service, improving threats detection or detection of fraudulent content/behaviour, improving the customer's support could constitute legitimate interests (cf. EDPB Opinion 28/2024). By contrast, using AI to optimize illegal drug smuggling operations would not serve a legitimate interest. Article 88c does not change the notion of legitimate interest, which is not predetermined by the use or not of AI (AI might be used for legitimate or for illegitimate interests).

Why are only some aspects relevant for the application of Article 6.1.f GDPR mentioned in Article 88c?

- Reference to aspects such as the data minimisation are specifically mentioned because of their relevance in the context of AI development. Recital 31 explains that all aspects of Article 6.1.f GDPR, such as the consideration of the reasonable expectations of the data subjects, must be met, as well as any other requirement of the GDPR.

119

GDPR: Processing in the context of AI

Why does the Commission state that enhanced transparency and the unconditional right to object in Article 88c are safeguards going beyond controller's obligations?

- For example, the right to object without providing reasons (unconditional) is not an obligation because Art 21(2) GDPR is limited to direct marketing. Enhanced transparency is the transparency going beyond what is required under Art 13 and 14 GDPR, such as for example, additional information about the data collection criteria, alternative forms of informing data subjects, e.g. media campaigns, FAQs, model cards (see EDPB Opinion 28/2024, para. 98 et. seq)

Why the rules under Article 9(2)(k) and Article 9(5) are not included in the AI Act?

- The GDPR is the main instrument of regulating data protection. The AI Act includes only rules in relation to specific aspects, i.e. it provides for a legal basis for the processing of special categories of data for the detection and removal of bias, in compliance with Article 9(2)(g) GDPR, and for the further processing of personal data in sandboxes.
- The exception of Article 9(2)(k) read in conjunction with Article 9(5) do not provide for a legal basis for processing. The controller must have to rely on a legal basis under Article 6 GDPR.

120

GDPR: Processing in the context of AI

What is the aim of the exception under Article 9(2)(k)?

- The aim of this exception is explained in recital 33. The AI development often relies on large amount of data, a phenomenon which is specific for AI, and despite all appropriate measures to be taken by the controller, special categories of data may still exist in the data sets or retained in the AI model or system. The exception seeks to not disproportionately hinder the uptake of AI while ensuring a high level of protection of personal data.
- The AI development and operation is not a purpose of processing. Art 9.2.k explicitly states "in the context of AI development and operation".
- Art 9(2)(k) and Art 9(5) address situations where the special categories of data are not necessary for the intended processing. This is explicitly explained in recital 33 and indicated in Art 9(5) which states that the controller must take all appropriate measures to avoid the processing of special categories of data. If those data were necessary, it would be contradictory that the controller must avoid the processing.
- The derogation respects the proportionality principle.

121

GDPR: Processing in the context of AI

Does Article 9(2)(k) create a broad exception?

- Art 9(2)(k) explicitly refers to the conditions set out Art 9(5). Read together, the exception is narrowly framed.
- The controller must meet a series of conditions: First, to take all appropriate measures to avoid the collection of special categories of data. Second, where despite such measures, special categories of data are residually processed, the controller must either remove those data or, where removal requires disproportionate effort, take other measures to effectively mitigate the impact the residually processed data may have on the rights of the data subjects.
- It follows the logic of other derogations under Art 9(2) by indicating certain safeguards or conditions of processing. All other requirements of the GDPR must be met.
- As for any other measures, compliance is supervised by the DPAs – see also EDPB Opinion 28/2024 in relation to processing of any personal data in AI models.

Does "remove" in Art 9(5) mean deletion of data?

- Removal of data has the usual meaning, i.e. deleting the data

122

GDPR: Biometric data processing

What scenarios does Art 9(2)(l) cover / which is its relation to other exceptions of article 9(2)?

- Art 9(2)(l) applies to any kind of biometric data, e.g. fingerprints, facial images, iris
- The exception covers scenarios of verification, e.g. access controls, subject to the condition that the biometric data or the means needed for the verification is under the sole control of the data subject. In EDPB Opinion 11/2024, the exception would cover Scenarios 1 and 2.
- The controller, instead of seeking the explicit consent of the data subjects under Art 9(2)(a) GDPR, may choose to apply this exception.

What is meant by "held solely by the data subject"?

- Recital (34) further explains that sole control requires that solely the data subjects hold, in a secure manner, the biometric templates or the means (e.g. decryption key) to access the templates.
- The sole control by the data subject ensures that the controller does not gain knowledge of the biometric data, or in any event it gains knowledge for the limited time of the verification process. Hence, any other use or further processing is not possible without the active involvement of the data subject.

123

GDPR: Automated individual decision-making

Why change the approach to a possibility with conditions? Does it affect the necessity test for the performance of the contract?

- Art 22 GDPR provides for conditions and safeguards that mitigate the risk of possible negative consequences of automated decision with legal or similarly significant consequences. This is also the intention of Convention 108+.
- The current wording allows for restrictive interpretation (by some authorities) that hinders the use of automated tools, including in areas of cybersecurity and fraud prevention or in pre-contractual phase to protect their and their client interest.
- The proposed changes do not affect the possibility of the individuals to ask for a review and contest such decision.
- They further clarify the threshold for necessity assessment in case of a contract.
- They bring a level-playing field for the use of such automated tools across the EU.
- All sectoral rules (consumer protection, anti-money laundering, payment services) enacted in compliance with Art 22 GDPR, remain unaffected.

124

GDPR: Controllers' information requirements

What is considered "non-data intensive"?

- As illustrated in recital 36, 'not data-intensive' is where the controller collects a low amount of personal data and the processing operations are not complex.
- Applies to controllers where the processing of personal data is not their core activity.
- To be read alongside the other requirements in Article 3(5). The examples in the recital refer to situation where the amount/number of categories of data processed are limited.

What is considered a clear and circumscribed relationship?

- Requires a direct relationship between the data subject and the controller.
- Objective is to cover interactions between an individual and small operators such as a local shop, an artisan such as a painter or a shoemaker, or a local sports club as is made clear in recital 36.

Why are the information exception requirements in Article 14 unchanged?

- Requires a direct relationship between the data subject and the controller so the exception is not included in Art 14 GDPR.

125

GDPR: Controllers' information requirements

Does the provision apply when sensitive data is processed such as in a doctor-patient setting?

- Provision applies when:
  - there is a relationship between the controller and the individual,
  - the processing is non data-intensive,
  - not likely to result in a high risk to the data subject, and
  - there are reasonable grounds to expect that the data subject already has the information.
- Unlikely that these requirements would be met in a doctor-patient setting.

How does this lead to simplification – does it reflect the risk-based approach?

- Proposal builds on the rules that are already in place: information obligation does not apply where the data subject already has the information set down in Art 13 (1)-(3) GDPR.
- The proposal reflects the risk-based approach of the GDPR.
- Should reduce the disproportionate burden placed on such entities where the processing of personal data is not their core activity.
- Benefits small operators.

126

GDPR: Exercise of the right of access

What is the rationale for introducing additional limitations only for the right of access. Does the proposal lower the level of protection for data subjects?

- The proposed amendment builds on the already existing framework that permits data controllers to refuse excessive access requests.
- Access requests are 'excessive' if the right is abused for purposes other than the protection of personal data.
- Rationale is to limit abusive right of access requests that place a significant burden on a controller when dealing with such requests.
- Reflects the abuse of rights doctrine which is well established by the CJEU.
- It does not lower the level of protection.

Protection against abuse already exists – why cannot the examples mentioned in the recital be relied upon using existing grounds? How will this impact supervisory authorities

- Intention is to provide legal clarity to controllers on lawful options to handle situations where access requests are clearly abusive.
- The rules on possibly abusive requests to supervisory authorities have not been amended in the Omnibus.

127

GDPR: Exercise of the right of access

What is meant by "data protection purposes"

- For right of access requests, excessive requests include the abuse of this right for purposes other than the protection of a data subject's personal data. The limitation must be read in light of the intention of abusing this right.
- Recital provides examples which includes requests where the data subject only intends to cause damage or harm to the controller or intends to essentially blackmail the controller for financial profit.
- For example, a data subject requesting their health records in order to be informed of test results could not be seen as abusing this right – there is no abusive intention.

Changes to the burden of proof

- What is considered "reasonable" in this context: "reasonable" is an already existing standard in the GDPR. Controllers already have to apply this standard in other areas of the GDPR – including in Art 12.
- Controllers bear the burden of proof and will still have to demonstrate that the request is excessive – see Art 3(4) last sentence.

128

GDPR: Data breach notifications 1

What are the benefits of COM adopting the list of circumstances of 'high risk' data breaches? Does this not affect the independence of DPAs/EDPB? How are specific national/regional contexts taken into account if a single definition of 'high risk' is adopted at EU level?

- The list of circumstances is a flexible and living tool: It does not as such provide for a definition of 'high risk' but indicates circumstances which should be taken into account when the data controller assesses the level of risk. The list is non-exhaustive and it will be regularly reviewed and updated as necessary.
- The adoption of the list by means of a COM implementing act provides for more legal certainty as such lists are then legally binding across the EU. This ensures more consistent notification practices in all MS and, as a result, more consistent enforcement of the GDPR.
- This approach also allows to take into account MS views and input before the adoption of the list. MS may consult their DPAs about possible adjustments to the draft list prepared by the EDPB when it is discussed in the examination procedure. The objective is to ensure that the lists are as practical and operational as possible.
- The draft list is prepared by the DPAs/EDPB in full independence and taking into account national experiences and practices, as appropriate.

129

GDPR: Data breach notifications 2

How is the level of data protection ensured following the new higher threshold for notifications? How is the risk of 'underestimated risks' mitigated?

- The high volume of data breach notifications even in low-risk situations undermines the overall efficiency of the GDPR. The simplification of notification obligation allows the controllers and GDPR enforcers to better focus on issues which may cause significant risks to data subjects.
- The common EU-level list of circumstances in which data breach is likely to result in a high risk (the new threshold for notification) and the common notification template provide legal certainty and minimise the risk of 'underestimated risks'. The list of 'high risk circumstances' ensures more consistent notification practices across the EU, including communication of data breaches to affected data subjects.
- The controllers continue to have the obligation to document all data breaches, including their effects and remedial action taken, and make such records available to DPAs. The controllers also continue to be obliged to be able to demonstrate, in accordance with the accountability principle (Art 5 GDPR), that the notification threshold is not reached, if they do not notify.
- The incentive for correct notification should be high due to potential administrative fines in the case of an infringement of the notification obligation and the data subject's right to compensation for the possible damage suffered as a direct result of the infringement of this obligation.

130

GDPR: Data breach notifications 3

The extension of the time limit to 96 hours – consistency with other EU digital legislation under SEP and effects on the protection of data subjects

- The proposal aims to facilitate compliance of smaller operators which have more limited '24/7 oversight and response' capacity (in particular during the weekends/public holidays).
- The objective of the single-entry point for incident reporting (SEP) is not to harmonise the time limits or criteria for reporting. The 96-hour time limit is GDPR-specific and addresses the challenges raised by stakeholders relating to reporting of personal data breaches.
- The time limit of 96 hours is a maximum time ('not later than'). It is likely to reduce the unvoluntary non-compliance with the required timeline causing additional administrative burden (para. 1 of Art 33 GDPR) and the need to rely on the possibility to 'provide information in phases without undue further delay' (para. 4).
- The incentive for swift notification of data breaches should be high due to potential administrative fines in the case of an infringement of the timeline and the data subject's right to compensation for the possible damage suffered as a direct result of the infringement of this obligation (including measures to mitigate possible adverse effects).

The amendment's effect on processors (paragraph 2 of Article 33)

- The new high-risk threshold (para. 1) applies automatically also to processors (para.2), in the same way as the current threshold of 'risk' applies to them. The processor continues to be obliged to notify the controller without undue delay after becoming aware of a personal data breach.

131

GDPR: Processing activities requiring and not requiring a Data Protection Impact Assessment

What are the benefits of COM adopting the blacklist and whitelist, template and methodology for conducting DPIAs? Does this not affect the independence of DPAs/EDPB? Does this not mean adopting a 'formalistic checklist undermining the risk-based approach'?

- The adoption by means of a COM implementing act provides more legal certainty as then the lists, templates and methodology are legally binding. This allows for a more harmonised and consistent application of the GDPR across the EU.
- This approach also allows to take into account MS views and input before the adoption of the lists.
- MS may consult their DPAs about possible adjustments to the EDPB draft lists etc. when they are discussed in the examination procedure. The objective is to make sure that the lists, template and methodology are as practical and operational as possible.
- The draft lists, template and methodology are prepared by the DPAs/EDPB in full independence and taking into account national experiences and practices.
- The adoption of lists at EU level does not affect the current nature of DPIAs. The lists are a flexible and living tool; they are *non-exhaustive* and regularly reviewed and updated as necessary. The controllers would still need to assess their processing activities on a case-by-case basis in light of the lists and – if not covered by the lists – considering the requirements of Art 35 GDPR to determine whether a DPIA is required/whether their processing is 'high risk'.

132

GDPR – additional questions

Why does Omnibus VII not cover corresponding amendments of the LED

- Report on the application of the LED to be adopted mid-2026.
- From a legal point of view, it is not possible to amend a Directive through a Regulation, except in very limited circumstances.
- Recital 41 states that the LED should be brought into alignment with amendments to the GDPR introduced under the Omnibus.

Is there an inconsistency between the GDPR, the DA and the DGA relating to international data transfers?

- The scope of these legislations are different. For transfer of personal data, the rules set under Chapter V of the GDPR is and remains the applicable framework.

Why has the COM decided not to define "health data" (Article 9 GDPR)?

- See Art 4(15) GDPR. The Digital Omnibus does not change this definition.

133

Cybersecurity

Single-entry point for incident reporting

134

Questions on financing and analysis of impact & costs

- Cost calculation methodology
  - **For companies**: under the assumption that 160 000 NIS2 entities (based on NIS2 data extrapolations) have to report 1.18 incidents per year with an average cost of 440 EUR per incident -> EUR 83 million/year. If reporting is reduced by 50% (to one instead of two authorities, e.g. for NIS2 and GDPR) = savings of EUR 41.5 million per year.
  - **For Member States**: building a national platform would cost on average EUR 550 000 per MS + additional maintenance costs of 2-4 FTE per MS.
  - **For ENISA** (budgetary implications under CSA2/ENISA mandate): initial development cost of EUR 6 million + EUR 500k for onboarding of any additional legal act + 8 FTE for maintenance (based on CRA SRP experience; see also ESAs Report under Art 21 DORA)

135

Questions on security of SEP

- **Safeguards that ENISA would ensure security**
  - Examples of such safeguards to be defined in the technical specifications could be:
    - a proper governance and relevant policies (defining e.g. the security objectives of SEP)
    - access and identity management
    - secure software development lifecycle in every development stage
    - Development, Security, and Operations (DevSecOps) Integration
    - risk and threat management
    - security testing and validation (e.g. scanning, pen testing)
    - vulnerability management
    - awareness and training
    - incident response and recovery
    - business continuity (backup management and disaster recovery)
    - ....
- **Measures to ensure the security and prevent a single point of failure**
  - Member States' authorities should ensure that they can receive incident notifications through alternative means (not prescribed), in the exceptional event that a technical impossibility prevents the submission of incident notifications using the SEP. This information should be publicly available *(recital 57)*.

136

Questions on security of SEP - the process

How would it be assessed when ready to onboard, what would be the process?

- Member States would be part of the process during all phases, i.e. in the design, development, piloting, testing and assessment before the SEP becomes operational:
  - ENISA to develop the technical, operational and organisational measures regarding the establishment, maintenance and secure operation of the SEP on the points listed in *Art 23a(3)* in cooperation with the MS (CSIRTs network and competent authorities) and COM
  - ENISA to consult competent authorities before piloting the functioning of the SEP (e.g. on the specificities and requirements for the notifications for a specific Union legal act that should be considered for the test)
  - COM to consult MS (CSIRTs network and competent authorities) on the proper functioning, reliability, integrity and confidentiality of the SEP (e.g. by consulting them on the assessment methodology and findings).
  - ENISA and COM to make use of existing cooperation groups and networks of Member States

137

Questions on security of the SEP and issue of trust

- Ensure trusted relationship between authorities and reporting entities
  - The aim of the comprehensive consultation process is to ensure that the SEP becomes a workable solution for MS.
  - To that end, MS should also advise ENISA and COM on their stakeholders perspective and needs to ensure that notifying entities have trust in the SEP and ensure a user-friendly experience.
  - The SEP should not affect trust building efforts between authorities and reporting entities and follow-up exchanges during incidents.
  - The SEP merely provides a tool/conduit to facilitate compliance with legal reporting obligations.

138

Questions on national security and EU competences

- Not changing any substantive requirements for any of the legal acts – channeling existing obligations (based on Art 114 TFEU)
- Digital Omnibus does not modify CER Art 1(8) or NIS2 Art 2(11) – no obligation to supply information, the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence
- Robust security safeguards for SEP required to be ensured

139

Questions on functionality and how it will work in practice (1)

Data storage & personal data:

- Digital Omnibus proposal does not change the current requirements regarding access to data
- Technical specifications will define in cooperation with MS the details and modalities (e.g. for retrieving/supplementing data, encryption of data, storage/routing of data)

Interoperability, interplay with existing solutions & languages:

- Recital 52 refers to continuity and interoperability with existing national technical solutions
- Technical specifications in cooperation with MS – MS will have a say on main elements

Reporting by group structures:

- Digital Omnibus does not modify the entity that must report incidents – e.g. existing NIS2 regime applies for NIS2, DORA for financial entities

140

Questions on functionality and how it will work in practice (2)

Communication between entity and CSIRT:

- SEP to enable this kind of communication (NIS2 Art. 23a(3)(b))

Alternative means:

- Not specified in Recital 57 - could be e.g. email or telephone, depending on existing national practices.

141

Questions on simplification, timelines, templates (1)

Reporting timelines & content:

- No modification to reporting timelines.
- Contents: Legal basis for CER & GDPR templates + existing legal basis for NIS2 templates + existing DORA templates (Imp. Reg. 2025/302) + eIDAS ? potential for streamlining (see also *Recital 54*)

Minimum harmonisation:

- Where type of information and format of notifications are not (fully) harmonised, MS to inform ENISA about national provisions. (*Recital 53*)

Information sharing between authorities:

- *Recital 55*: SEP could be built to accommodate subsequent sharing of information between authorities.
- No legal obligation to use SEP for such information exchange.

142

Questions on simplification, timelines, templates (2)

Timeframe of SEP development:

- ENISA shall develop the SEP within 18 months from the entry into force of the Digital Omnibus Regulation.
- ENISA shall pilot the functioning of the SEP for each added Union legal act.
- COM, in cooperation with ENISA, shall assess the proper functioning reliability, integrity and confidentiality of SEP.

  If positive assessment – COM publishes a notice; SEP ready to proceed.

  If not positive assessment – ENISA, in cooperation with COM, shall take corrective measures without undue delay. COM reassesses and publishes notice.
- The obligations to report via the SEP enter into application 18 months from the entry into force of the Digital Omnibus Regulation.
- When COM finds in its assessment that the SEP does not ensure the proper functioning, reliability, integrity or confidentiality, term of application can extend to 24 months.

143

Questions on simplification, timelines, templates (3)

Is it necessary to harmonise CER and GDPR templates?

- The idea is to streamline the contents of reported information to the extent possible, ensuring consistency, promoting synergies and reducing administrative burden on entities by minimizing the number of data fields that entities are required to complete.

144

Questions on interplay with other legislation

- **Inteplay with CSA revision**
  - The forthcoming proposal for a revision of the Cybersecurity Act will address the mandate of ENISA, reflecting the new task in relation to the SEP.
  - The new CSA will include proposals to further simplify compliance with cybersecurity obligations.

- **Integration of NCCS or aviation rules – when and how?**
  - Given that the cybersecurity-related incident reporting obligations in the network code on cybersecurity aspects of cross-border electricity flows and the relevant instruments for the aviation sector arise from delegated and implementing acts, their inclusion in the SEP requires amendments to these respective delegated and implementing acts.

145

146