Council of the European Union
General Secretariat

Brussels, 01 December 2025

Interinstitutional files:
2025/0359 (COD)
2025/0360 (COD)

WK 16586/2025 INIT

LIMITE

SIMPL
ANTICI
DATAPROTECT
CYBER
TELECOM
CODEC
PROCIV

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 1 December)

Delegations will find enclosed a presentation as prepared by the Commission for the meeting of the Antici Group (Simplification) on 1 December regarding the Digital Omnibus package (Omnibus VII).

European Commission

DIGITAL OMNIBUS

Q&A session

Antici Group on Simplification

01/12/2025

Cybersecurity

Single-entry point for incident reporting

1. Single entry-point for incident reporting

Multiple cybersecurity (horizontal and sectorial) and other relevant rules (data protection, physical resilience) require incident reporting – NIS2, GDPR, eIDAS, CER, DORA. The **same event** may be required to be reported to different authorities in various Member States, according to different templates.

Issue: duplication of effort, administrative burden & cost on companies.

Effects:

- May discourage from reporting incidents.
- Potential lower compliance rate across relevant legislation & less meaningful info shared as part of reporting due to burden of multiple channels.
- Reduces overall resilience - companies focus on complying with incident reporting obligations instead of incident mitigation.
- Reported data not comparable.
- Potentially less effective info sharing among various relevant authorities.

Costs and Benefits

Consultation findings

Industry called for a **"report once-share many"** (CSA revision public consultation, stakeholder submissions, Implementation Dialogue on Cybersecurity, focus groups, calls for evidence).

According to an ECSO study, 82% of surveyed entities reported that they have to notify more than one authority in case of a cybersecurity incident, with 21% of respondents stating that they had to notify 5 authorities.

Costs

Costs for single-entry point borne by ENISA (to be secured for ENISA mandate); **minimal cost for companies** (training staff to use a new interface).

Benefits

- Allows companies to **focus on response** to cyber incidents and **ease workload** on IT security departments, without compromising the information needs of authorities.
- **Better reporting rates**, potentially more meaningful and coherent content.
- **Rationalisation of reporting obligations** and reduction of administrative burden.
- With the conservative estimate that the single-entry point can reduce the reporting costs by 50%, it would result in approx. **EUR 41.5 million of savings each year** – calculation based only on 160 000 NIS2 entities. Expected that it would cut reporting by up to 80%.

Single entry-point for incident reporting – what is it

- **Single-entry point** to support the obligation to report incidents and related events under various legal acts
- Mandate use for reporting under **NIS2, GDPR, DORA, CER, eIDAS**
- **ENISA** tasked to develop and maintain the single-entry point
- **Secure-by-design**
  - ENISA to *take* ***appropriate and proportionate technical, operational and organisational measures*** *to manage the risks posed to the security of the single-entry point and the information submitted or disseminated via the single-entry point*.
  - **At a second stage: Technical specifications done in cooperation** with **Commission, CSIRTs Network and MS authorities** as per the relevant acts.
  - **Possibility to integrate national solutions (Recital 52)**
  - Companies can retrieve and supplement information - allows reporting in various stages
  - Where relevant, link to the **Business Wallets**

Single entry-point for incident reporting – timeline and developments

- **Piloting/testing prior** to onboarding – Commission, after **consultation of the CSIRTs network and the competent authorities** under the Union legal acts to assess the functioning
- Timeline - 18 months from DO entry of into force + max 6 months delay in case of functionality issues
- May build on the Cyber Resilience Act (CRA) single reporting platform; needs to ensure that it serves the specific requirements and needs of each specific legislation
- Streamline **contents of incident reports/templates, as relevant.**

Single entry-point for incident reporting – what is it **not**

- No substantive changes to current requirements under the respective acts.
- No changes on recipient authorities, their roles or competences.

Incident reporting templates

- New empowerment for template under GDPR: New Article 33(6)
  - EDPB „shall prepare and transmit to the Commission a proposal for a common template for notifying a personal data breach […] The Commission after due consideration reviews it, as necessary, and is empowered to adopt it by way of an implementing act […].”
- New empowerment for template under CER Directive: New Article 15(2)
  - “The Commission may adopt implementing acts further specifying the type and format of information notified […]”
- Recital 54: “Regulation (EU) 2022/2554 has introduced standardised reporting templates streamlining the content of reports for major ICT-related incidents for the financial sector. The experience gained from the adoption of these templates provides valuable insights and best practices that should be taken into account when specifying the type of information, the format and the procedure of a notification for the purposes of reporting to the single-entry point under Directive (EU) 2022/2555, Directive (EU) 2022/2557 or Regulation (EU) 2016/679, where appropriate… This approach aims to ensure consistency, promote synergies and reduce administrative burden on entities by minimizing the number of data fields that entities are required to complete, thereby facilitating more efficient and streamlined reporting processes”

AI

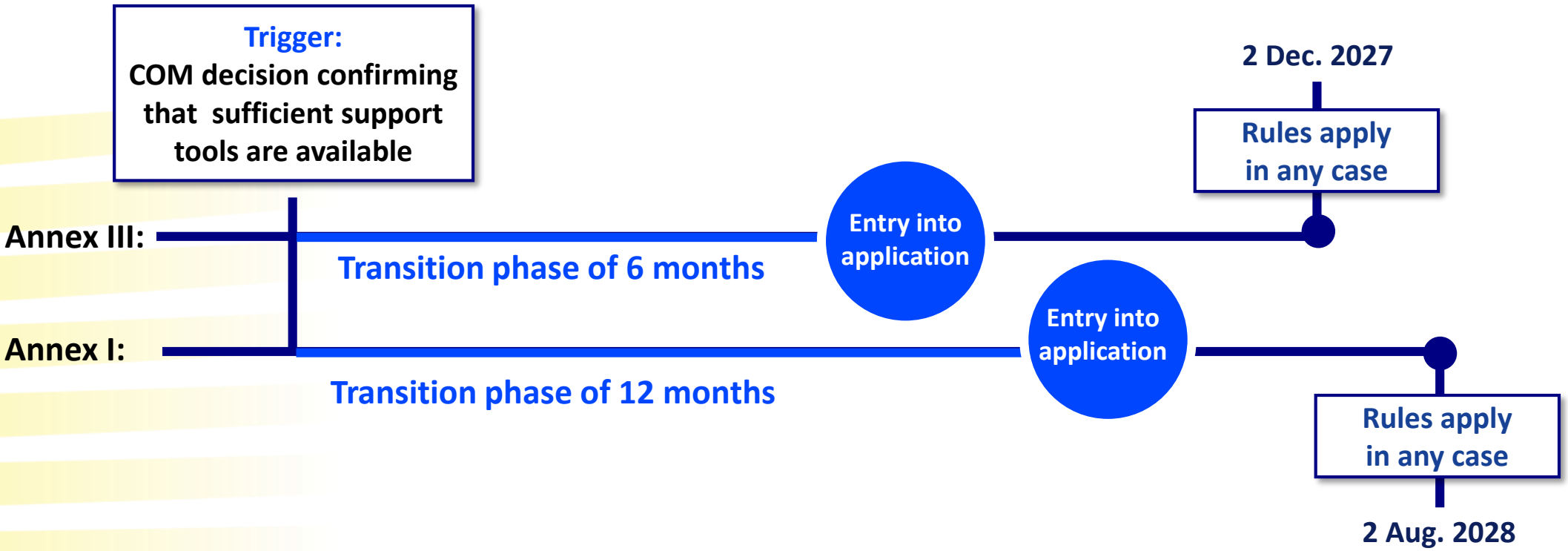
Amendments to the AI Act

2. AI Act

1. Timeline for high-risk AI rules (Article 113)

- Objective of COM proposal is to link the entry into application to the availability of support tools that offer legal certainty, rather than set a fixed date
- Support tools could be harmonised standards, common specifications or Commission guidelines
- Conditions for decisions are not specified to allow some flexibility (e.g. to use the ‘trigger’ if individual standards are at different stages of finalisation)
- COM decision is the legally correct and procedurally fastest choice for the ‘trigger’
- End date is a safeguard by which the rules apply in any case – whether harmonised standards, common specifications or guidelines are fully available or not

Timeline for high-risk AI: how does it work?



2. AI Act

2. Extended scope of powers for AI Office (Article 75)

- AI Act already foresees that GPAI systems built on GPAI models should be supervised by the AI Office if offered by the same provider (Article 75(1) AI Act); proposed changes to scope:
  - Clarification that AI Office powers cover all AI systems by the same provider as the GPAI model
  - Exclusion of high-risk AI systems covered by Annex I AI Act from AI Office supervision
  - Extending AI Office supervision to cover AI systems embedded in very large online platforms and search engines under the Digital Services Act
- Growing number of AI systems being built on GPAI models (see p. 80 SWD), require particular technical expertise that is already built-up in AI Office
- Proposed Article 75(1) AI Act creates legal basis for cooperation with national authorities, will be detailed in implementing acts; intended as assistance of national authorities to COM similar to implementation of competition law (e.g. to carry out on-site investigations)
- COM vision for cooperation in AI Act and DSA enforcement services is set out in recital 15

2. AI Act

3. AI Regulatory Sandboxes (Articles 57, 58)

- EU-level AI Office sandbox concerns AI systems under its supervision (i.e. based on GPAI models and AI systems that constitute or that are integrated into VLOP/VLOSE)
- Proposed amendment creates a possibility for the AI Office to establish an AI regulatory sandbox, COM intends to set this up in 2028
- Amendments to Article 57 and 58 AI Act will strengthen the coordination between national sandboxes, not create further obligations for MS in creating and operating sandboxes
- Deadline for creating MS sandboxes is not postponed – they are a key compliance enabler role in helping providers (especially SMEs and SMCs) to prepare and assess compliance with the requirements

2. AI Act

4. Extension of real-world testing (Articles 60, 60a)

- New Article 60a is less detailed than Article 60 because the sectoral rules for AI systems falling under Annex I Section B significantly differ
- Creating common rules would be very difficult and it is also important to retain flexibility to take into account the particularities of the sectoral rules
- That is also why Article 60a introduces voluntary agreements

2. AI Act

5. Legal basis for processing of special categories of data for bias detection and mitigation (Article 4a)

- New Article 4a extends the legal basis for the processing of special categories of personal data for bias detection and mitigation to non-high-risk AI systems and AI models (for providers as well as deployers)
- Conditions to use the legal basis (previously in Article 10(5) AI Act) and safeguards are not changed, only the scope of the provision
- New provision must be in Chapter I of the AI Act, since it would no longer be applicable only to high-risk AI systems
- Terminology is adjusted from ‘strictly necessary’ to ‘necessary’: this amendment aligns the threshold with the existing approach in the EU data protection law for processing special categories of personal data; strong safeguards remain in place

2. AI Act

6. Transformation of AI literacy obligation (Article 4)

- Experience since the entry into application shows that there is significant concern around Article 4 AI Act due to its lack of clarity; companies incur high compliance cost, on top of existing spending on staff training (p. 70, 72, 78 SWD)
- Transformation leads to an encouragement, not an enforceable obligation
- Deployers of high-risk AI systems have an obligation to ensure that their staff is trained to perform effective human oversight (Article 26(2) AI Act)
- COM continues to very actively support AI skills with actions launched under AI Continent Action Plan, Apply AI Strategy & other initiatives
- Regulatory exchange and harmonisation of national approaches in AI Board

2. AI Act

7. Registration of ‘filtered’ AI systems (Article 6(4), 49(2))

- Only providers of high-risk AI systems have to register those systems in the EU database, the change aligns to this default rule
- Market surveillance authorities are competent to supervise all AI systems and can intervene if necessary, including upon complaints (Article 85 AI Act)
- AI Act includes two safeguards to ensure traceability and avoid overly broad application of ‘filter’:
  - (1) Documentation obligation in Article 6(4) AI Act
  - (2) Special procedure in Article 80 AI Act
- AI Act does not specify the format of documentation according to Article 6(4) AI Act, further guidance could be considered

2. AI Act

8. Fundamental rights protection authorities (Article 77)

- More authorities can be designated, because this is no longer limited to obligations protecting fundamental rights related to high-risk AI systems in Annex III (i.e. related to prohibitions & transparency)
- Requests for access to documentation have to be channeled through market surveillance authorities, to avoid that companies face duplicative request and reduce burden (& it may even be faster)
- Without prejudice to existing rights to request information or documentation under the laws that the authorities supervise (e.g. GDPR)

2. AI Act

9. Extending regulatory privileges to SMEs (Article 63) and SMCs (Articles 11, 17, 70, 95, 96, 99)

- Introducing definitions for SMEs and SMCs; no need to define start-ups because they are a subset of SMEs (‘SMEs, including start-ups’)
- Nature of simplified compliance pathways in Article 11, 17 and 63 AI Act has not changed, only the type of company they apply to
- Simplified compliance with Article 63(1) AI Act ‘only’ extended to SMEs because it is already possible to set up the quality management system a way that acknowledges size (Article 17 AI Act); important to consider that the risk of an AI system does not depend on the size of the provider

2. AI Act

10. Single application procedure for notified bodies (Article 28, 29)

- Aims to reduce the procedural burden on conformity assessment bodies that want to be designated as notified body under the AI Act and a sectoral law
- Applies only where such a single application and single assessment procedure is also foreseen in sectoral law; applied sector-by-sector
- Procedure only changes the application to become a notified body, not the competences required nor the monitoring of notifying authorities
- COM is preparing guidance on the requirements for notified bodies under Article 31 AI Act

2. AI Act

11. Transition period for notified bodies (Article 43(3))

- Objective is to ensure availability of notified bodies when rules start to apply
- No obligation for notified bodies to apply the transitional rule
- Supervision of sectoral notified bodies by the sectoral notifying authorities is up to the sectoral law; transitional rule of the AI Act only requires that the applicable requirements in Article 31 AI Act are fully checked
- Transitional period is not a substitute of designation, the notified bodies have to eventually be designated after the period expires

2. AI Act

12. Including Article 17 in conformity assessment (Article 43(3))

- Despite being placed in Chapter II, Article 17 is one of the AI Act's essential requirements for high-risk AI systems
- References in other parts of the text clearly show that Article 17 AI Act is intended to be covered by the conformity assessment, for example Article 43 Act refers to Annex VII (Conformity assessment based on assessment of quality management systems and assessment of technical documentation)
- COM has requested a standard to be developed for the quality management system (C(2025)3871), which will facilitate conformity assessments

2. AI Act

13. Establishment of NANDO Codes

- Approach to development NANDO Codes pursues 3 objectives:
  1) ensuring full coverage of high-risk AI systems subject to third-party conformity assessment
  2) being sufficiently granular as to allow conformity assessment bodies to seek notification for a limited set of systems
  3) limiting the number of necessary codes for simplification purposes
- COM considered two key elements: (i) infrastructure necessary to assess conformity (e.g., symbolic AI will require standard servers and low compute while GPAI will require high computer and large GPU clusters); and (ii) the categories of professional skills required to assess conformity
- Notified bodies can be notified under various technology-specific codes at the same time (even all codes)
- Proposed NANDO codes do not overlap or substitute designations and corresponding codes under the Union harmonisation legislation

2. AI Act

14. Removal of empowerments for implementing acts

- COM set itself a target to adopt harmonised conditions for the implementation only where strictly necessary
- Proposal would remove 4 empowerments for implementing acts that were found not to meet this condition:
  - Articles 50(7) and 56(6): approval of Codes of practice (based on experience with General-Purpose AI Code of Practice)
  - Article 72(3): harmonised template for post-market monitoring plan, based on stakeholder feedback
  - Article 69(2): proposing a procedurally less complex procedure aligned to the conditions set out in Implementing Regulation (EU) 2025/454

Data

GDPR

3. GDPR

Definition of Personal Data

- **The proposed new definition does not change the notion of personal data.**
- **This definition builds on recital 26 GDPR as clarified in the recent *SRB* case-law.**
- **The recital and the case-law already stated that data should not be considered personal data when the entity does not have the means reasonably likely to be used to identify the natural person concerned by the data.**
- **The new definition merely brings legal certainty by codifying this standard in the operative part of the GDPR.**

3. 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;**
  - **Clarify the condition of compatible processing;**
  - **Clarifies that legitimate interest can be basis for scientific research;**
  - **Extend the exceptions from the information obligation for processing in case of scientific research under certain circumstances.**
- **These amendments will help the scientific community to use personal data to achieve their research goals.**
- **The conditions and safeguards of Article 89 GDPR remain unchanged.**

3. GDPR

Personal data processing in the context of AI development and operation

- **Proposed amendment clarifies the current GDPR rules: a controller may rely on Article 6.1.f for pursuing a legitimate interest in the context of AI development and operation, where all conditions of that provision and the other GDPR requirements are met.**
  - **It does not create a new ground for lawful processing; the development and operation of AI does not per se qualify as legitimate interest.**
  - **It reflects EDPB Opinion 28/2024.**
- **Article 88c and recital (31) lists in a non-exhaustive manner measures and safeguards to address risks in the context of AI development and operation**
  - **e.g. technical indications embedded in a service limiting the collection of data for AI development.**
- **Enhanced transparency and the unconditional right to object are meant as safeguards going beyond the controller's obligations.**
- **The definitions ensure consistency with the AI Act.**

3. GDPR

Processing of special categories of data in the context of AI development and operation

- **Proposed amendment sets out a narrow exception, following the logic of Article 9(2). It does not amend Article 9(1) nor affects the other GDPR requirements; the controller must comply with all other rules.**
- **Proposed amendment applies where all of the following are met:**
  - **the controller does not aim to process special categories of personal data (to note: if the aim is to process special categories, controller must rely on another derogation under Article 9(2);**
  - **the controller has taken all appropriate measures to avoid processing of special categories of data during the AI life-cycle;**
  - **despite such measures, special categories of data have been collected or retained in the AI model/system (=residually processed), in which case the controller should remove those data or, where this is disproportionate, take other measures which effectively protect the data subjects.**

3. GDPR

Biometric data processing

- **Proposed amendment fully aligns with the definition of biometric data (Article 4(14)) and in Article 9(1), as explained in recital (51) GDPR.**
- **The EDPB has consistently considered the functions of biometric identification (1:many matching) and verification (1:1 matching) as processing of special categories of data.**
- **Proposed amendment provides for a narrow exception from the prohibition in certain instances of biometric verification, i.e. where the data subjects remain in sole control.**
  - **Recital (34) 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.**
- **Proposed amendment does not change the rule that biometric are personal data which undergo processing by a specific technical means.**
  - **For example, there is no change regarding where photographs are considered processing of special categories of data.**

3.2 GDPR

Automated individual decision-making

- **The objective is to make the provision clearer by moving from a prohibition with exceptions to a possibility with conditions.**
- **As a prohibition, in certain instances it was interpreted very restrictively, impeding its use even where necessary safeguards were in place.**
- **Clarifies the use of automated decision making in the context of contracts is not disqualified only because the decision could be taken by humans (instead of automated means).**

3. GDPR

Controllers' information requirements

- **The proposed amendment builds on the rules that are already in place.**
- **It exempts controllers from providing certain information to a data subject where:**
  - **there is a relationship between the controller and the individual, (so Article 14 is out of scope)**
  - **the processing is non data-intensive,**
  - **not likely to result in a high risk to the data subject, and**
  - **where there are reasonable grounds to expect that the data subject already has the information.**
- **It benefits small operators (e.g. artisans, sport clubs)**
- **Non-data intensive activities are those where the controller collects a low amount of personal data and its processing operations are not complex. The scope of the processing must also be limited to the minimum data necessary to perform the service.**

3. GDPR

Exercise of the right of access

- **The proposed amendment builds on the existing framework to limit abuses of the right of access to personal data.**
- **It specifies for right of access requests that they are ‘excessive’ if the right is abused for purposes other than the protection of personal data.**
- **For example, where the requesting data subject only intends to cause damage or harm to the controller or intends to essentially blackmail the controller for financial profit.**
- **The controller bears the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive.**

3. GDPR

Mechanism to give greater legal clarity on anonymisation and pseudonymisation techniques

- **The Commission may adopt implementing acts to specify means and criteria for pseudonymising data that no-longer constitutes personal data for certain recipients.**
- **Controllers will be able to use these means and criteria as element to demonstrate that data cannot lead to re-identification of data subjects.**
- **Close involvement of the EDPB.**
- **Controllers are not exempted from the responsibility to comply with the GDPR.**
- **The objective is to help businesses by establishing clear conditions when data resulting from pseudonymisation can be presumed to be non-personal data.**
- **This will create legal certainty and reduce the compliance cost.**

3. GDPR

Data breach notifications

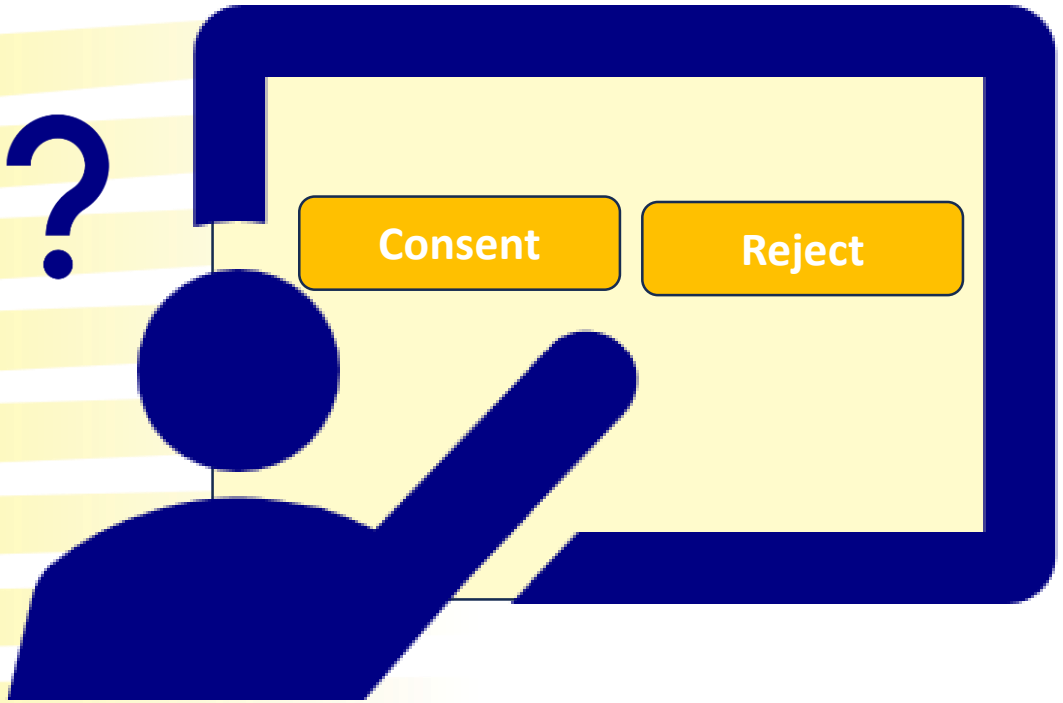
- **The common EU list of ‘high risk data breaches’ provides legal clarity to controllers and ensure more consistent notification practices, including the communication of data breaches to affected data subjects.**
- **The adoption of the list and templates for data breach notifications by way of an implementing act provides more legal certainty to controllers as such act is legally binding.**
- **The extension of the notification period from 72 to 96 hours responds in particular to a request from smaller operators, also addressing the issue of weekends.**
- **The obligation of controllers to document any data breaches continues to apply.**

3. GDPR

Processing activities requiring and not requiring a Data Protection Impact Assessment

- **The objective is to harmonise the lists of activities requiring DPIAs and not requiring them to ensure a consistent application of Article 35 GDPR.**
- **The adoption of the lists by way of an implementing act provides more legal certainty to controllers as such act is legally binding.**
- **The preparation of the proposals for the lists remains with the EDPB/DPAs and they may continue to do so in complete independence and building on national practices.**

Cookie rules



- Users today are faced with multiple cookie consent pop-up requests. This causes **fatigue**:
  - Pop-up banners are **complex, often multilayered and repetitive.**
  - Pop-up banners **do not inform**: Users find it hard to understand what their consent is being asked for.

  ⇨ Users click away banners **without making an informed choice**

- Pop-up banners are **costly for businesses**: EUR 400 per year and website.

3. Cookies

Scope of carve out in Article 5(3) ePD and Article 88a 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, creating a single regime.**
- **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.**

3. Cookies

Consent requirement and exemptions from consent

- **The high level of protection for citizens' rights to privacy and protection of their personal data must be safeguarded → consent requirement remains**
- **Exemptions from consent are narrow and for low-risk purposes; maintain the high level of protection.**
- **Proposal introduces a "whitelist" of low-risk processing purposes that are exempted from consent requirement.**
- **Given the narrow scope, exemptions apply to the access and the subsequent processing: processing is lawful.**

3.Cookies

Tackling complex cookie banners to reduce consent fatigue

- **Pop-up banners are complex, often multilayered and repetitive.**
- **This causes cognitive burdens and fatigue**
- **The Omnibus proposes a set of measures that controllers need to respect when requesting data subject's consent when accessing their devices.**
- **Data subjects must be able to refuse processing with a single click.**
- **The refusal must be respected for at least 6 months.**
- **Data subjects will be able to set their preferences centrally and have that choice respected**
- **The principles of the GDPR and in particular the requirements for consent (Art 7 GDPR) remain fully valid.**

3. Cookies

Automated machine readable indications for consent preferences

- **Repetitiveness of consent requests via cookie banners and the lack of understanding what consent is solicited for are key drivers of cookie consent fatigue.**
- **Facilitating data subjects to make their choices centrally (e.g. in a browser) can address this fatigue and reduce the numbers of banners.**
- **Commission will request development of standards to facilitate the application of the rules.**

3. Cookies

Automated machine readable indications for consent preferences

- **Repetitiveness of consent requests via cookie banners and the lack of understanding what consent is solicited for are key drivers of cookie consent fatigue.**
- **Facilitating data subjects to make their choices centrally (e.g. in a browser) can address this fatigue and reduce the numbers of banners.**
- **Commission will request development of standards to facilitate the application of the rules.**

3. Cookies

Media services

- **Media providers have an important role for democracy.**
- **Media services providers need to be able to reach their audience, allowing to ask for consent directly from individuals.**
- **Exemption from the obligation to respect a signal transmitted through automated means indicating consent preferences of a user ≠ exemption from asking consent.**

Data

Data Act

Four to one

Data sharing of IoT data (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

3. Data Act
Free Flow of Non-Personal Data Regulation

Challenges

Voluntary actions on cloud switching have been superseded by Data Act.

Complex supervisory model for data localisation requirements.

Further provisions that have not been relevant in practice.

Solution

Repeal of the Free Flow of Non-Personal Data Regulation and integrate only the Regulation's central Article (prohibition of unjustified data localisation requirements in EU) into the Data Act.

Benefits

Leaner legal landscape (**one instrument out**)
Repeal of outdated rules

3. Data Act

Rules on data intermediation services

Challenges

Current legal framework (Data Governance Act) overly prescriptive – inhibited the development of data intermediation services.

Solution

Sharper definitions.

Conditions for obtaining the label more flexible – in particular the strict legal separation with other services.

Regime becomes voluntary (label).

Benefits

Greater uptake leading to **more voluntary data sharing or pooling,** e.g. in the context of common European data spaces.

3. Data Act

Role of competent authorities & complaints

The intention of the proposal is not to change substantially the public enforcement of the instruments brought under the Data Act.

3. Data Act

Role of the European Data Innovation Board

- **The proposal does not alter the character of the EDIB as a consultative body to the Commission, similar in function to a Commission expert group. No decision-making power is foreseen. It merely coordinates the enforcement and serves as a forum of discussion for the development of a European data economy and data policies.**
- **The changes allow the involvement of political decision-makers in complement to the enforcement authorities.**
- **EDIB shall not be competent for the enforcement of chapter VI of the Data Act – as is currently the case.**

3. Data Act

Deletion of Article 36: “Essential requirements regarding smart contracts for executing data sharing agreements”

- **Deleting Article 36 means developers no longer need to (re)design smart contract used for data sharing agreements with specific requirements (e.g. interruption or archiving functions).**
- **Generally speaking, smart contracts remain a highly promising tool to foster secure, transparent and efficient data sharing, including in the context of the Data Act.**

3. 1 Data Act
Rules on data altruism organisations

Challenges

Current legal framework (Data Governance Act) overly prescriptive and ineffective – inhibited the registration of data altruism organisations and put reporting burden on MS.

Solution

Sharper definitions.

No more mandatory 'data altruism rulebook'.

No more reporting obligation for MS about national arrangements for data altruism.

Benefits

Greater uptake leading to **more altruistic data sharing**

Reporting burden **reduction** for MS

A single, streamlined instrument for re-use of public sector data

Challenges

Two instruments (DGA/ODD):

- Different definitions
- Uncertainty which regime applies when (eg in case of anonymization)

Market balances: Small entities find it harder to re-use data.

Solution

Merge the rules into Data Act – streamline where possible, keep separate where necessary.

Clarify definitions and scopes.

New rules allow public sector bodies to set out different rules for very large enterprises.

Benefits

Consolidated rules & clear scope for **easy re-use.**

Harmonized framework for re-use – without touching on national access regimes.

Fighting reinforcement of dominant market positions, **ensuring fairness.**

3. 1 Data Act

New structure for the new framework for the re-use of public sector information

Complementary instruments with overlapping provisions.

Aim: Streamline where possible, keep separate where necessary.

- **Section 1:** Scope and common principles (eg principle of non-discrimination)
- **Section 2:** Rules of the former Open Data Directive
- **Section 3:** Rules of the former Chapter II Data Governance Act on protected data (includes documents)

3. 1 Data Act

Special conditions for very large enterprises

- **Re-use of public sector data benefit a wide range of market participants and should not inadvertently reinforce existing dominant positions.**
- **Very large enterprises, and in particular undertakings designated as gatekeepers under Regulation (EU) 2022/1925, hold significant power and influence over the internal market.**
- **Special conditions for very large enterprises are a measure to support fair competition and innovation.**
- **Public sector bodies may set out special conditions, e.g. higher charges and fees for the re-use of open government data and protected data.**
- **Such conditions must be proportionate and based on objective criteria, taking into o consideration economic power and the entity's ability to acquire data**

3. 1 Data Act

Narrowing down Chapter V on business-to-government (B2G) data sharing obligation only to public emergencies

- **Revised Chapter V eliminates the need for companies to prepare for vague 'exceptional need' circumstances. The B2G data-sharing obligation only applies to 'public emergencies'; the definition remains unchanged.**
- **General clarification of the provisions in Chapter V.**
- **EU and Member State public sector bodies (including statistical bodies) can continue to rely on the Data Act to obtain the data they need to address public emergencies.**

3. 1 Data Act

Consultations in support of the proposed amendments

- We have conducted a wide consultation of stakeholders with focus on European businesses and in particular SMEs, with hundreds of replies.
- 1 public consultation
- 1 implementation dialogue with European SMEs and civil society organisations
- 2 reality checks with European SMEs and civil society organisations
- SME panel

- The reports of these exchanges are annexed to the Staff Working Document

3. 1 Data Act

Timeline

- The aim of the amendments is to bring immediate reliefs to businesses and citizens alike. They are of technical nature – focus on streamlining and clarifying existing rules.
- To achieve this, the technical amendments should enter into force as soon as possible after their adoption, with a simultaneous entry into application.

Platform-to-Business Regulation

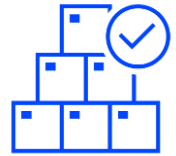
Simplification measure

Repeal of the P2B Regulation

Maintain provisions that are cross-referenced by other acts:

- Selected definitions
- Statements of reasons & complaint mechanism

Timeframe until 2032 to amend other acts relying on P2B



Benefits

Reduced compliance costs due to layered and overlapping rules. Online intermediary service providers will benefit from increased **clarity of legal provisions**.

More coherent and robust enforcement vis-à-vis larger platforms, by clearly identified regulators, avoiding potential duplications.

4. P2B

- To what extent do DSA and DMA cover P2B provisions?

GOAL: ensure transparency for business users

- **Measures on terms and conditions are covered by the DSA for all recipients of platforms of all sizes**
- **Measures on ranking and self-preferencing are covered by the DSA for platforms of all sizes (except micro and small) and by the DMA for gatekeepers**
- **Measures on access to data covered by the DMA for gatekeepers**

GOAL: ensure fairness by online platforms

– **Obligation to ensure mediation and complaints covered by the DSA for platforms of all sizes (except micro and small) and by the DMA for gatekeepers**

4. P2B

- Will business users continue to be protected?

  - **Business users continue to benefit from complaint-handling systems and mediation offered by online platforms**
  - **Self-employed platform workers will continue to benefit from P2B transparency measures on restriction, suspension and termination**
  - **Business users will continue to have the right to representative action**
  - **Enforcement of maintained P2B provisions remains; DSA and DMA enforcement for repealed P2B provisions**

4. P2B

- How can fragmentation be prevented?

  - **Not a vacuum: e-Commerce Directive, DSA and DMA are of full harmonisation covering intermediary services and online platforms**
  - **EUCJ caselaw**
  - **Very narrow space for national measures**