European Commission

PUBLIC

DIGITAL OMNIBUS

Digital Simplification Package

Antici Subgroup on Simplification

21/11/2025

Simplification and political objectives

- **New 2024-2029 Commission mandate**: simplification as a support tool to EU competitiveness.
- October 2025 **Council Conclusions** called for "further ambitious simplification packages", "including on digital".

The Digital Omnibus is the seventh of such packages. EUR 5 billion in administrative cost savings are expected for businesses by 2029.

The Digital Simplification Package

Europe has pioneered **digital regulation** and has set high standards for protecting fundamental rights, consumer safety and our values. Clear, coherent rules are key to **effective implementation**.

This Package delivers **fast and visible improvements** for people and businesses, and triggers a more **cost-effective, innovation-friendly** implementation of European rules.

Cutting all redundancies, **unnecessary compliance costs** and **reducing reporting obligations** Stimulating **business opportunities** and supporting **competitiveness**.

The package of measures

Digital Omnibus

Data Union Strategy

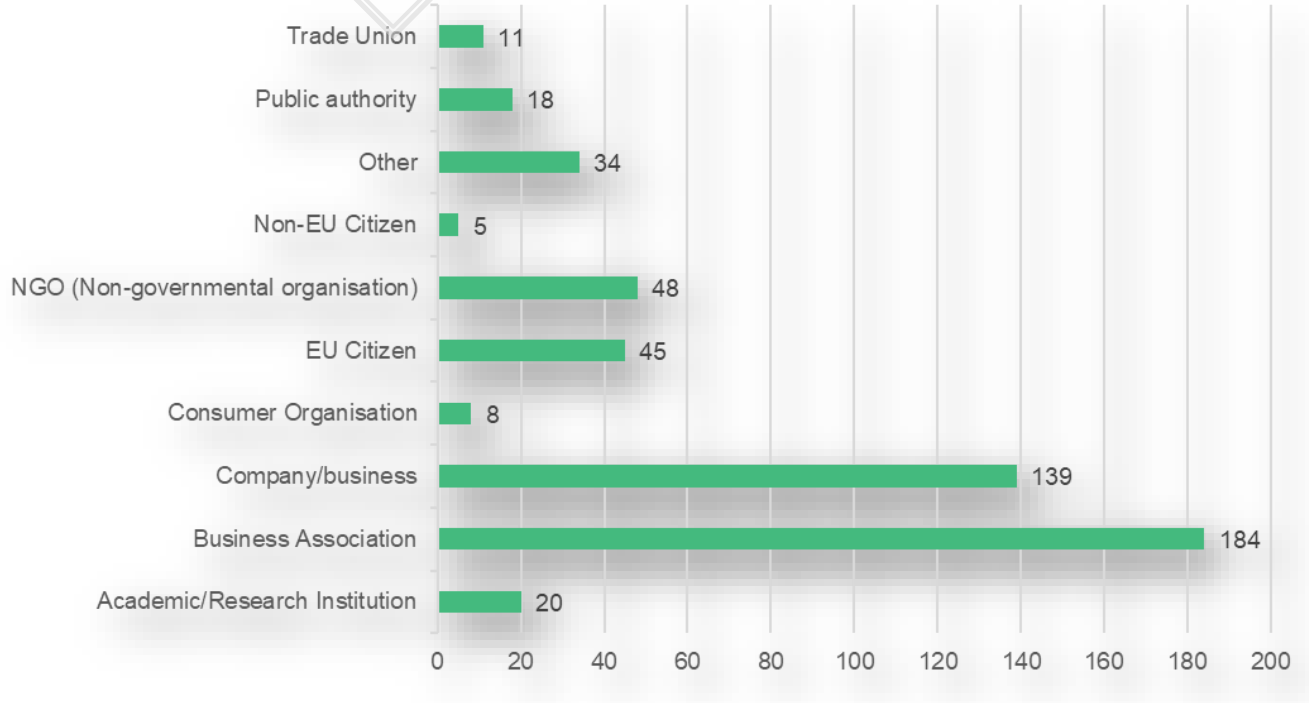
EU Business Wallet

Digital Fitness Check

Consultations and supporting analysis

- **3 public consultations**, on the AI, cybersecurity, and data pillars of the Digital Omnibus
- A **Call for Evidence** on the Digital Omnibus
- **Implementation dialogues** and **reality checks**
- An **SME Panel**

- All supporting analysis to the initiative can be found in the **Staff Working Document** to the Digital Omnibus.



Breakdown of responses: Call for Evidence on the Digital Omnibus

Digital Omnibus - Outline

Amendments to rules in course of application

Artificial Intelligence Act

Data acquis

Incident reporting: cybersecurity

Repeal of the P2B Regulation

Amendments to rules already applicable

I. Simplification of the AI Act

A clear, effective and innovation-friendly roll-out of the AI Act, through:

- **Addressing implementation challenges**
- **Reducing cost & simplifying compliance with the AI Act**

In addition to existing support measures like Codes of practices, guidelines, stakeholder outreach & the AI Act Service Desk

Alignment of implementation timeline

Challenges

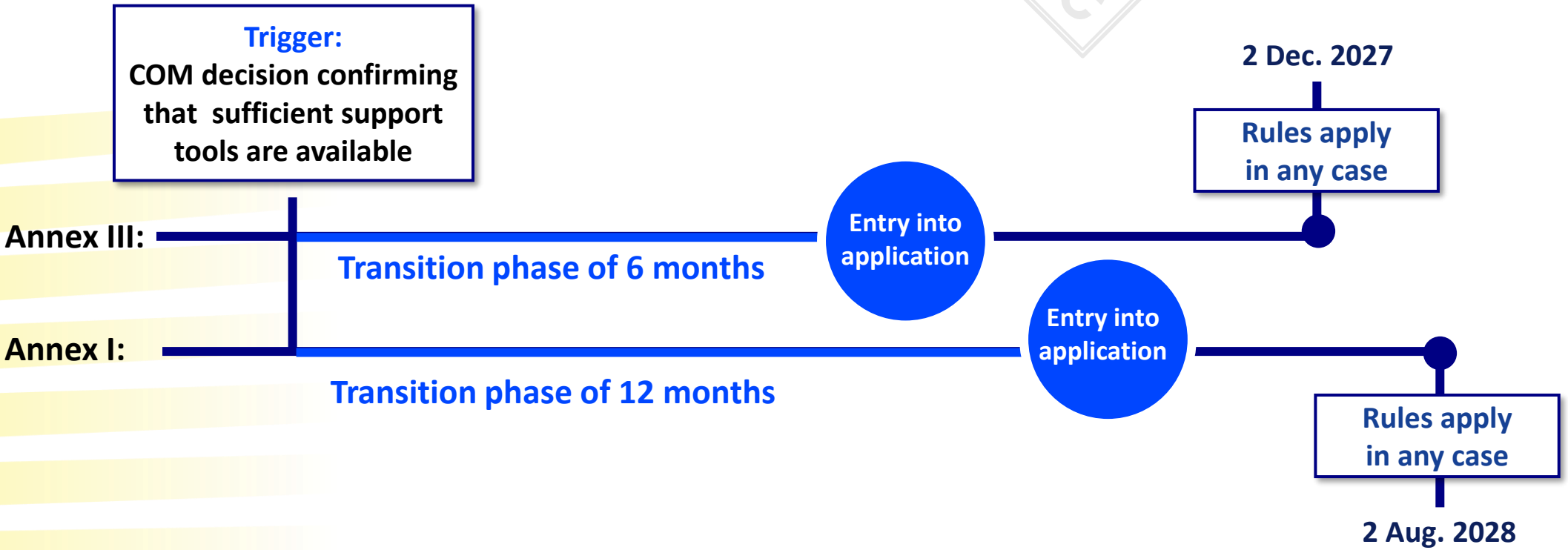
Delay of standards causes legal uncertainty.

Delay of national authorities impedes preparation.

Simplification measures

Alignment of timeline for rules of high-risk AI systems.

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



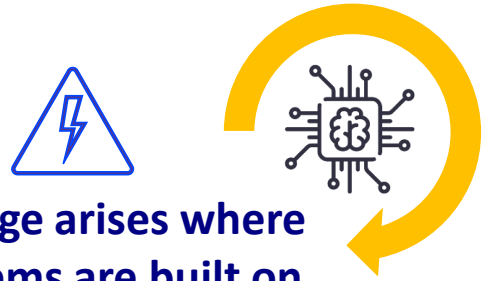
Improving effectiveness of supervision

AI Act oversight follows a two-tiered approach:

Oversight of AI systems rules by national authorities

Oversight of general-purpose AI (GPAI) models by AI Office

Challenge



Challenge arises where AI systems are built on GPAI models

- Omnipresence of applications built on GPAI models & growing overall number.
- Technological development in field of AI agents.
- Lack of technical experts.

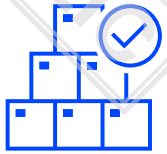
Simplification measure

Clarify that the AI Office's powers extend to <u>all AI systems built on GPAI models</u> by the same providers (e.g. ChatGPT) and extending it to AI systems embedded in VLOPs/VLOSEs.

- **Using synergies from AI Office's expertise in GPAI model supervision.**
- **Reducing exchanges of information between different governance layers.**
- **Fostering coherent application of AI system rules.**

Simplifying burdensome obligations

Challenges



Simplification measures

Challenges	Simplification measures
Compliance cost is very high for small businesses with limited legal resources.	Extending simplified compliance to SMEs (Art. 63) and SMCs (Art. 11, 17, 70, 95, 96, 99).
Horizontal AI literacy obligation (Art. 4) causes concerns due to vagueness.	Replacing AI literacy obligation for companies by an obligation on MS and COM.
Registration burden not justified for AI systems that are not high-risk (Art. 49(2)).	Removing registration for AI systems that are exempted from being high-risk.
Providers need flexibility in post-market monitoring of high-risk AI systems (Art. 72).	No harmonised conditions through implementing act, but voluntary guidance.

Measures to facilitate compliance

Facilitating compliance with EU data protection laws by allowing providers and deployers of all AI systems and models to process special categories of personal data for bias detection and correction, subject to appropriate safeguards.

Fostering cross-border use of AI regulatory sandboxes and facilitating the set-up of an **EU-level AI regulatory sandbox.**

Broader use of real-world testing for high-risk AI systems for sectors, including offering the possibility for voluntary agreement between COM and MS.

Simplifying procedures for notified bodies

Challenge	Simplification measure
Duplication of administrative burdens in designating notified bodies under the AI Act and other EU legislation.	Creating single application and assessment procedure.
Risk of a gap in availability of notified bodies when the rules start to apply.	Establishing a transitional rule to ensure availability of notified bodies.
Determining the scope of the designation of notified bodies lacks a common approach.	Establishing the so-called NANDO codes to facilitate the classification of notified bodies.

II. The Data Acquis

Data Union Strategy

Digital Omnibus: Data Act

Digital Omnibus: General Data Protection Regulation

Digital Omnibus: cookies rules

Data Union Strategy – unlocking data for AI

Pillar 1: Scale up access to high-quality data for AI and innovation

The strategy will support **greater data sharing** across the EU economic fabric and **unlock new business and technological opportunities** for European innovators.

Pillar 2 – Simplify the data regulatory landscape

Using the Digital Omnibus as a legislative vehicle, the strategy will make data rules **simpler, clear and more cost-effective** for businesses.

The Commission will also **support companies** in the implementation of the Data Act.

Pillar 3 – Adopt *an open but assertive approach* to international data flows

To strengthen Europe's global position, the strategy will operationalise our '**open but assertive**' approach to international data flows – to **attract** more flows in the EU while **safeguarding** the EU's data interests abroad.

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

Simplification of the GDPR

The proposed amendments aim to **harmonise, clarify, and simplify** the application of the GDPR - while continuing to ensure a **high-level of data protection** across the EU.

They will **facilitate operators' compliance with the GDPR and support technological innovation in the EU,** including the development of European AI.

The proposed changes also **benefit data subjects by ensuring a more uniform application of the GDPR** and by bringing clarity to key GDPR concepts.

The amendments are based on a continuous dialogue with stakeholders over the last number of years, and in particular the Implementation Dialogue on the application of the GDPR that took place on 16 July.

Consultations and rationale

- The core message from stakeholders was that they consider the GDPR as a balanced legal framework which has met its objectives. Overall, there was **no call for a general reopening** of the GDPR.

- However, there were calls for some targeted amendments to **further harmonise** the application of the GDPR and **to simplify controller obligations.**

- The proposed amendments also **reflect recent significant judgments** from the Court of Justice of the European Union as well as **opinions from the European Data Protection Board** (EDPB).

- The amendments do not affect the GDPR core principles and requirements.

Definition of personal data

Challenges

Lack of clarity as to when an individual is “indirectly identifiable”, and therefore whether the GDPR applies.

Solution

Clarify the definition of personal data in relation to pseudonymised data (Article 4), reflecting the case law of the CJEU (SRB case).

Benefits

Bring clarity reflecting recent **CJEU case-law**.

Increase legal certainty for operators where pseudonymisation techniques are used.

Processing activities requiring and not requiring a Data Protection Impact Assessment (DPIA)

Challenges

Fragmentation due to different national lists by DPAs on when a DPIA is required.

Only a few national lists on when DPIAs are not required.

Solution

Establish lists at EU level on when DPIAs are required, and on when DPIA are not required.

EDPB prepares a proposal for a common template and methodology for conducting a DPIA.

Implementing act by COM.

Benefits

Provide legal certainty to controllers by reducing fragmentation in the requirements of conducting a DPIA and clarifying the notion of “high risk”.

Data breach notifications

Challenges

Data breach notifications to supervisory authorities in low-risk situations is considered unnecessarily burdensome.

Lack of clarity as to when a breach is considered to pose a 'high risk' to data subjects .

Solution

Notification only of high-risk breaches.

Extension of the deadline to 96 hours.

EDPB prepares a proposal for common notification template and a common list of "high risk" breaches.

Implementing act by COM.

Benefits

Reduce controllers' **administrative burden**.

Ease the notification process through a single channel.

Alleviate the workload of supervisory authorities.

Harmonise at EU level the **notion of "high risk"** for data breaches.

Personal data processing for AI development and operation

Challenges

Lack of clarity on whether legitimate interest can be relied on to process personal data in the context of the development and operation of AI.

Solution

Clarify that personal data may be processed for a legitimate interest in the context of development and operation of AI under Article 6 (1)(f) GDPR where relevant conditions are met and subject to additional safeguards

Provide an exception for the processing of special categories when it is only residual and subject to specific safeguards.

Benefits

Support **innovation and development of European AI,** while maintaining a **high level of data protection**.

Controllers' information requirements

Challenges

Controllers' information obligations considered disproportionate where there is a low risk to the data subject and where they already have the relevant information in practice.

Solution

Exempt controllers from providing certain information to a data subject where the processing is 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.

Benefits

Benefits e.g. **small operators** (e.g. artisans, sport clubs) that carry out low-risk data processing to whom information obligations may cause a disproportionate burden.

Ease the information obligations of controllers in situations where it brings no added value to the data subjects.

Personal data processing for scientific research

Challenges

Lack of clarity in the research community regarding the conditions for GDPR compliant scientific research.

Solution

- Provide a definition of scientific research.
- Clarify that scientific research constitutes a legitimate interest.
- Clarify the compatibility of further processing.
- Provide for appropriate safeguards where information directly to the data subject is impossible or disproportionate.

Benefits

Support **research and innovation** in the EU.

Exercise of the right of access

Challenges

Situations where the right of access is used by data subjects in an abusive manner for purposes other than the protection of their personal data.

Solution

Clarify where the right to access to one's personal data is used by data subjects in an abusive manner, for purposes other than the protection of their personal data.

In such circumstances, the controller may either refuse to act on the request, or ask for a reasonable fee for replying to the request.

Benefits

Provide legal clarity to controllers on how to handle situations where **access requests** are clearly **abusive**.

Allow controllers to focus on genuine **access requests**.

Automated individual decision-making

Challenges

Unclear in which situations a controller can use automated individual decision-making.

Solution

Clarify when decisions based solely on automated processing are permitted.

Benefits

Provide greater legal certainty to controllers regarding when they can lawfully make **use of automated individual decision-making.**

Biometric data processing

Challenges

Unclear distinction between the functions of identification and confirmation of an individual's identity (verification) based on biometric data.

Solution

Provide for an exemption when processing of biometric data is necessary for verification and the data subject has the sole control.

Benefits

Bring clarity to when **biometric data can be processed to confirm the identity of a data subject.**

Support **innovation** while maintaining a high level of **protection.**

Mechanism to give greater legal clarity on anonymisation and pseudonymisation techniques

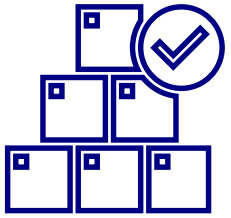
Challenges

Companies need to assess case-by-case when data are anonymous (non-personal) for a certain recipient -> very resource-intensive.

Solution

Give companies clearer guidance on how to generate data that are non-personal for certain recipients.

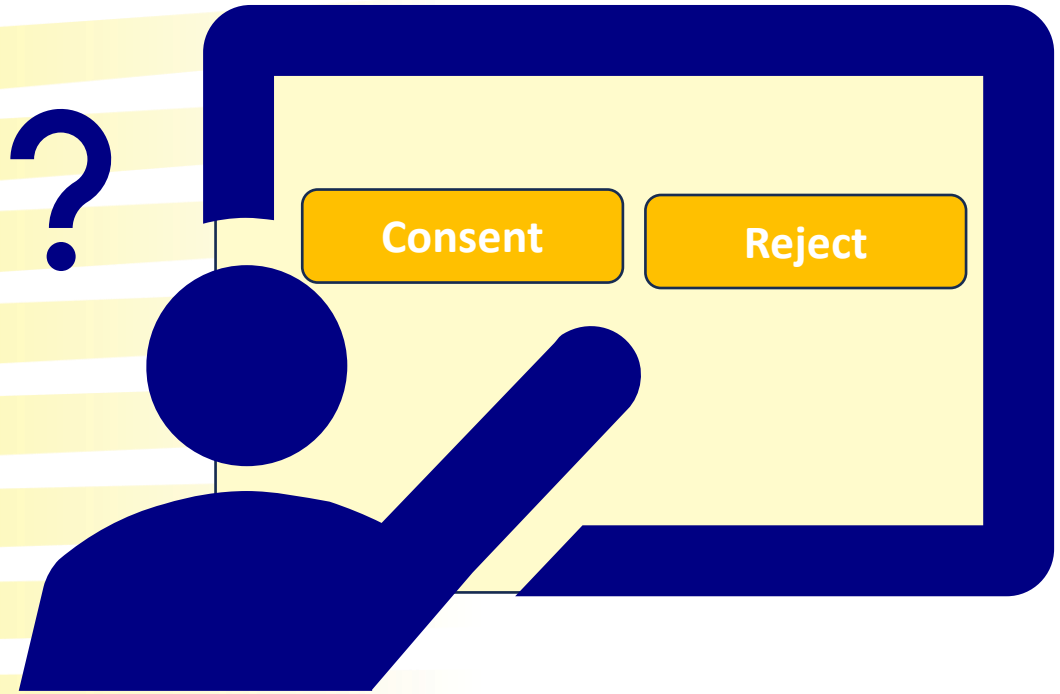
The Commission may adopt Implementing Acts with close involvement of EDPB.



Benefits

Companies have **lower cost** when aiming to generate **data meant to be anonymous** for certain recipients.

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.

Simplification measures

Challenges

- Frequent and complex cookie pop-up banners.
- "Cookie banner" fatigue.
- Feeling of not having meaningful choice.
- Feeling that only consent gives sufficient control and protection for a personal device
- Consent also required for low-risk processing.

Solutions

- Place rules under **GDPR** where personal data is collected.
- Maintain the principle that **access** to a device requires **consent.**
- Extend current consent exemptions for certain **low-risk purposes**.
- Cookie refusal is **respected for 6 months.**
- Allow for centralised cookie preference settings (e.g. in browser or other technical means) - with **exemption for media** services provider

III. Cybersecurity 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.

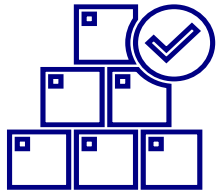
Issue: duplication of effort, administrative burden & cost on companies.

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.

Single-Entry Point

- Creation and use of a **single-entry point (SEP)** for reporting incidents/data breaches across different legal acts – NIS2, GDPR, DORA, CER, eIDAS.
- **No de-regulation,** maintaining a **high level of cybersecurity.**
- **No substantive changes to current requirements**.
- Streamline **contents of incident reports/templates, as relevant.**



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.**

Operationalisation

Uniform conduit for companies to report incidents and data breaches under multiple frameworks

Not a data processing platform: ENISA not accessing information unless provided so by the relevant acts

To be built, operationalised (in 18 months) and maintained **by ENISA**

Multi-authority (recipients are the respective competent authorities, CSIRTs and relevant recipients under each act)

Secure-by-design (avoid single point of failure) – technical specifications **in cooperation** with Commission, CSIRTs Network and MS authorities as per relevant acts; **piloting/testing prior** to onboarding

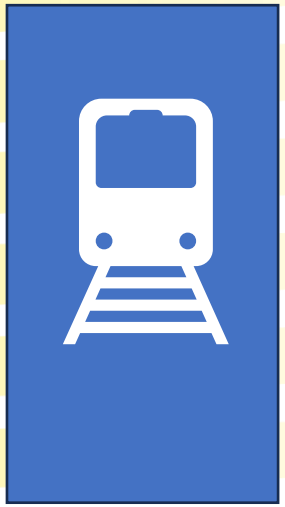
Allows reporting in various stages – companies can retrieve and supplement information

SEP may build on the Cyber Resilience Act (CRA) single reporting platform

Aim to ensure the continuity and interoperability with **existing national technical solutions**, as applicable

Reporting with SEP

Ransomware attack on a railway undertaking leading to a disruption of services and exfiltration of personal data



GDPR: Notification of a personal data breach

NIS2: Reporting of a significant incident

Single entry point

NIS2 competent authorities

Data Protection Authority

Other relevant competent 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

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%.

IV. Platform-to-Business Regulation (P2B)

- **First step** in 2019 to regulate the platform economy.
- Precursor to the Digital Services Act (**DSA**) and Digital Markets Act (**DMA**).
- Rules for online platforms are **now more robust** with DSA (2024) and DMA (2023).

→ Transparency

→ Fairness

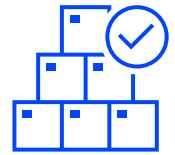
Simplification measure

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.

Looking ahead: Digital Fitness Check

Objective

Analysis of the digital rulebook and signal simplification potential. Emphasis on **coherence** and **cumulative effects.**

Join the conversation

Kick-off: mapping impacts and scoping the analysis.

Public consultation by 11 March

Timeline

Planned **adoption** of the Digital Fitness Check in Q1 2027.

PUBLIC