Digital Package

General questions

What is the digital package?

The Commission's digital package is designed to help EU businesses innovate, scale, and save on administrative costs. It includes a digital omnibus simplifying rules on data, cybersecurity, and AI, accompanied by the Data Union Strategy, and a proposal for European business wallets. These components aim to unlock high-quality data for AI and ease digital paperwork, reflecting the recommendations in the Draghi Report (https://commission.europa.eu/topics/competitiveness/draghi-report_en) to boost productivity through innovation in digital, addressing barriers to regulatory compliance, boosting access to high-quality data across Europe and delivering European business wallets to simplify business operations across the EU.

What are the main elements of the package?

The main elements of the package include a digital omnibus that proposes amendments to our personal and non-personal data and cybersecurity rules and certain elements of the AI Act. It also encompasses a Communication on the Data Union Strategy, model contractual terms on data access and use, and standard contractual clauses on cloud computing contracts, as well as a Regulation for European business wallets. Additionally, the package features a public consultation on the digital fitness check.

Why is the Commission proposing an omnibus legislation on digital rules?

The Commission aims to boost tech competitiveness and save money for EU businesses by simplifying rules, streamlining procedures, offering one-stop solutions, and removing overlaps and outdated provisions. This approach eases compliance, reflects digital sector needs, and unlocks innovation opportunities without compromising the protection of European citizens' and businesses' rights.

How will businesses benefit?

Top ten benefits:

1. Small and medium-sized enterprises (SMEs) and small mid-cap companies (SMCs) will be able to save money and time thanks to specific rules in the Data Act and the Artificial Intelligence Act and voluntary trust-marks for data intermediation services instead of regulatory obligation;
2. Simpler, streamlined rules on data, with targeted clarifications. We will have two laws, not five: the Data Act and the General Data Protection Regulation (GDPR);
3. Better protections for companies' trade secrets against potential leakage to third countries and clarification and focusing of rules where businesses need to share data with public authorities to emergency situations in the Data Act;
4. Added clarity on 'pseudonymisation' of personal data, showing that data protection requires diligence, but is not a barrier to innovation: with the new rules, after appropriate treatments to protect the individuals' identity, data sets can be shared and used under clear conditions;
5. Clearer rules on how to handle personal data when developing AI systems and models and in the context of scientific research and innovation;
6. Simpler cookie requirements and 'whitelist' of harmless purposes for which business do not need to ask users for

consent;
7. Support measures in the application of the AI Act, aligning obligations with availability of standards;
8. Innovation opportunities in developing trustworthy AI, with EU-sandboxes and real-life testing facilities;
9. European business wallets to identify, authenticate and exchange data in a secure and user-friendly way with public sector bodies. ease forms, compliance interactions with authorities;
10. Streamlining the reporting obligations in case of cyber incidents through a single-entry point.

How will consumers benefit?

Top five benefits:

1. **Citizens remain in control**: they decide when their devices can be accessed for placing cookies
2. **Simpler online navigation**: no more clicking five times in a maze of forms just to keep a shopping cart updated while shopping online. Revamped, user-friendly design for cookie choices, with one-click consent;
3. **Better enforcement for consumers' rights**: rules on access to terminal equipment when personal data is processed are moved from the ePrivacy Directive to the GDPR. This means fines for up to 4% of annual turnover of a company that trespasses consumer's device without agreement;
4. **Clearer protections when consumers' personal data is used for training AI**: clarifications of what is expected from companies when using personal data in their AI training to safeguard citizens' interests;
5. **More effective enforcement of the rules that protect and empower citizens online**: with the AI Office taking over the supervision of the AI systems and models used by very large platforms and search engines under the AI Act, the Commission can align enforcement priorities and ensure a more coherent and impactful supervisory strategy across both the AI Act and the Digital Services Act.

How will companies benefit from the proposals today in concrete numbers?

Both large and small companies across the EU will benefit from the simplifications in the omnibus, as well as European business wallets.

If all companies take up European business wallets, we estimate that EU businesses could see savings of up to €150 billion annually. Meanwhile, simplification measures proposed in our data, AI and cyber legislation are predicted to bring additional one-off savings of up to €5 billion between now and 2029.

These measures will not only put more money in the pockets of businesses but will also open up opportunities for innovation and growth, and reduce regulatory burdens.

For example, by presenting one unique business identity and a single channel of correspondence with governments across the EU, European business wallets reduce the hassle of complying with 27 different regimes.

Meanwhile, proposals to update our rules on data and AI and the introduction of a Data Union Strategy will unlock access to high-quality and fresh datasets for AI for innovation potential of businesses across the EU.

1. Digital Omnibus - Data rules

What are the main changes this omnibus is bringing when it comes to the EU's data laws?

Today's digital omnibus simplifies the EU's data laws, turning regulatory compliance into a competitive advantage, not a costly burden for EU's businesses.

It consolidates all data rules into only two major laws: the Data Act, and the General Data Protection Regulation, which remains central. It also proposes targeted amendments to help businesses overcome practical obstacles to boost access to data, as a key resource to fuel innovation, continuing to promote the highest level of protections for the rights and interests of citizens, and of privacy and trade secrets.

For the Data Act, the Omnibus proposes to:

- Target exemptions to cloud-switching rules for SMEs and SMCs and for providers of custom-made data processing services;
- Remove mandatory registration and label for data intermediation service providers, fostering growth by lowering

entry barriers to the market of data intermediation services;
- Reduce complexity of the data altruism framework to make sharing data for the public good easier;
- Consolidate rules on data held by the public sector, to support EU data-driven innovation;
- Limit and clarify the scope of the business to government sharing provisions to ensure that governments can have sufficient data in emergency situations (e.g. in cases of massive floodings or a pandemic) while not putting extra burdens on companies to share their data for situations that are not related to emergencies. The Commission expects to bring annual savings of around €20 million for companies and reduce legal uncertainty and compliance costs.

For the GDPR, the Omnibus proposes to:

- Modernise 'cookies rules': Users remain in control of who can access their device, with a **one-click consent** and central settings of preferences for how they want their data to be shared and processed. Updates to the 'cookies rules' will alleviate cookie banner fatigue with a simpler design that allows users to make real choices, and will generate more than €800 million in savings for businesses annually;
- Provide legal clarity and reduce the compliance burden for businesses, creating new opportunities to create value on top of personal data while keeping intact the core principles of the GDPR. For example, the amendments frame the legitimate use of personal data for training AI models, making sure users' interests are thoroughly considered and protected. They also codify recent case law on how personal data sets can be safely turned into data that can be shared with third parties without disclosing the identity of the data subjects. The measures are accompanied with strong safeguards to ensure that personal data of citizens remain protected at the highest level.

What are the changes to the scope of cloud-switching obligations?

The proposal would clarify the temporal scope of the Data Act's provisions to facilitate switching cloud providers. This targeted exemption would be limited to cloud services that are 'custom-made' or are provided by small and medium enterprises or small-mid caps (companies with less than 749 employees) and based on contracts signed before the Data Act's entry into application.

This is expected to result in around €1.5 billion in one-off savings for eligible cloud providers that would avoid costly and complex contract re-negotiations to bring them into compliance with the provisions on cloud switching.

How are we addressing cookie banner fatigue?

Currently, citizens are faced with countless cookie pop-up banners asking for consent when they visit a website. They find it difficult to understand what they are being asked to consent to and what happens to their data. As a result of this complexity and the sheer amount of pop-up banners, users often click on any button, just to be able to access the visited site. This is not a real choice made by citizens to protect their phones or computers and to choose what happens to their data.

Today's proposal modernises the 'cookies rules', with the same strong protections for devices, allowing citizens to decide what cookies are placed on their connected devices (e.g. phones or computers) and what happens to their data. The new rules give real choices to users, with simplified design and effective design requirements for asking for consent or for allowing users to refuse it. They also prepare the ground for technological solutions that will bring further simplification and central controls for users.

The proposal also simplifies the rules for businesses and media services, proposing a 'whitelist' of situations benign for users' privacy but valuable for the provision of services, such as statistics and aggregated audience measurements.

The proposal absorbs the rules under the GDPR and its strong protection framework. Any infringement to users' rights can now lead to a fine of up to 4% of the global turnover of the company.

How will the proposed reform on cookies benefit users and citizens?

The proposed reform package puts citizens back in control of their online choices:

- **Users have the control**: Access to terminal equipment based on users' consent
- **One click to say yes or no – and make it count**: Citizens can refuse all cookies with a 'single-click'. Cookie banners will need to make this possible by including a 'single-click' button. Websites must respect citizens choices for at least six months.
- **Simple, central control**: People can set their privacy preferences centrally – for example via the browser - and

websites must respect them. This will drastically simplify users' online experience.
- **Stronger enforcement, stronger rights**: The GDPR framework will apply to cookie rules, ensuring harmonised enforcement and meaningful sanctions against violations.
- **No banners for harmless uses**: Cookies used only for non-risk purposes - like counting website visits - will no longer trigger consent pop-ups. Less annoyance, more trust.
- **Better user experience, same strong protection**: The reform cuts meaningless clicks without weakening safeguards. Citizens gain genuine control, backed by the GDPR's robust protections.

What changes are proposed to the General Data Protection Regulation?

The Commission is proposing amendments to provide legal clarity and reduce the compliance burden for businesses when it comes to the GDPR.

Among other things, the proposal will:

- Clarify the definition of personal data while keeping the highest level of protection of personal data;
- Encourage the development and use of responsible AI solutions by giving legal clarity on the use of personal data for AI;
- Simplify certain obligations for businesses and organisations, for instance by clarifying when they must conduct data protection impact assessments and when and how to notify data breaches to supervisory authorities.

The protection standards for citizens and their personal data will be fully upheld. All measures are accompanied by strong safeguards.

How will personal data be redefined in this revision?

The Digital Omnibus proposal codifies a recent judgement of the Court of Justice. With the new rules, datasets can be shared and used, provided that the third party receiving the datasets does not have the ability to reidentify the individual. The data controllers who pseudonymised the dataset continues to bear all the obligations under the GDPR.

Further, given the rapid pace of technological evolutions, but also the variety of capabilities that companies may have to pseudonymise or to reverse the pseudonymisation of data, the Commission will be able to issue implementing acts to reflect this evolution. This should bring further legal certainty for businesses, and ensure up to date, robust protections for citizens' rights.

What do the new rules say on the use of personal data for AI?

Under the GDPR, the entity responsible for the processing of personal data may lawfully process personal data for "legitimate interest". The proposal clarifies how this applies to AI systems.

In line with the EDPB Opinion (https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en), personal data can be processed for AI models as long as any use in a specific situation does not break any EU or national law, and that the processing complies with all requirements of the GDPR.

The proposal submits this processing to strong safeguards and ensures that data subjects have the unconditional right to object to the processing of their personal data.

How will I be informed of the use of my personal data?

Under the GDPR, controllers do not have to provide information to individuals on how they're using their personal data again, if the individual already received this information. The proposal would extend this exemption when there are reasonable grounds to assume that the individual already has this information.

This change will benefit small operators, such as crafts persons that use personal data to contact their clients or sport clubs informing their members of upcoming activities.

Individuals continue to have the right to request information on the processing of their personal data.

2. Digital Omnibus - Cybersecurity rules

Why is the Commission simplifying cybersecurity incident reporting?

So far, the obligations to report cybersecurity incidents have created significant burden on organisations across the EU. Entities in the midst of responding to cyber incidents are currently obliged to submit obligatory reports under multiple legal acts, such as the Network and Information Security Directive (NIS), General Data Protection Regulation (GDPR), the Digital Operational Resilience Act and others. This may discourage timely or comprehensive reporting.

Hence, we are introducing a single-entry point through which entities can submit a report to simultaneously cover all their incident reporting obligations. This will not only cut the burden on entities but also boost cybersecurity by speeding up and streamlining the reporting process. For a large majority of organisations, this new single-entry point will cut the reporting effort in half.

What is the single-entry point and how will it be managed?

The single-entry point will allow to submit notifications via a single interface and ensure that a single piece of information can simultaneously contribute towards fulfilling an entity's reporting obligations under multiple Union legal acts, where these require the notification of comparable and often overlapping information.

The Digital Omnibus proposes that reporting under the single-entry point is mandated under the Network and Information Security Directive 2 (NIS2 Directive), GDPR, the Digital Operational Resilience Act Regulation, the Critical Entities Resilience Directive and the EU Digital Identity Regulation. In a second stage, other sector-specific rules in the energy or aviation sector would also be brought under the single-entry point.

The European Union Agency for Cybersecurity, ENISA, will be tasked to establish and maintain the single-entry point for reporting, which will build on the ENISA's experience gained from the single reporting platform under the Cyber Resilience Act. The introduction of the single-entry point will not modify existing reporting obligations or the authorities designated as recipients of such reports. ENISA or the Commission will not have access to the reported information, unless provided so by the respective legislation.

3. Digital Omnibus - AI Act

Why is the Commission proposing to amend the AI Act?

The AI Act entered into force on 1 August 2024. It follows a staggered entry into application, with some parts already applicable such as certain prohibitions, AI literacy, and rules for general-purpose AI models. Other parts of the Act are set to apply on 2 August 2026 and 2 August 2027.

This progressive roll-out allows us to build on the experience gathered in applying the first part of the rules. The Commission is committed to continuously learn and stepping up its efforts. This is particularly important in the context of a fast-evolving technology like AI.

Stakeholder consultations throughout 2025 revealed implementation challenges that need to be addressed so that the AI Act can be successfully rolled-out. This proposal puts forwards legislative amendments to that effect and complements ongoing efforts to facilitate compliance with the AI Act, like the launch of an AI Act Service Desk.

What are the main changes proposed to the AI Act?

The Commission is committed to a clear, simple and innovation friendly implementation of the AI Act, as set out in the AI Continent Action Plan and the Apply AI Strategy. Today's proposal brings the AI Act in line with this approach by:

Linking when rules apply to the availability of support

- Linking the application of the rules for high-risk AI to the availability of support tools like standards. The Commission is adjusting the timeline for the application of high-risk rules to a maximum of 16 months.

Introducing simplification:

- Extending certain simplified modalities of fulfilling the legal obligations from SMEs to small mid cap companies (SMCs), such as simplified technical documentation;
- Requiring the Commission and Member States to foster AI literacy, and ensure continuous support to companies by building on existing efforts (such as the AI Office's repository of AI literacy practices (https://digital-strategy.ec.europa.eu/en/library/living-repository-foster-learning-and-exchange-ai-literacy)) instead of enforcing unspecified obligations on operators, while keeping training obligations for high-risk deployers in place remain.
- Removing the prescription of a harmonised post-market monitoring plan, giving businesses more flexibility;
- Reducing the registration burden for AI systems used in high-risk areas for tasks that are not considered high-risk.

Improving the effectiveness of the AI Act's governance:

- Centralising the oversight of AI systems built on general-purpose AI models with the AI Office, to reduce governance fragmentation for developers of these models and systems;
- Concentrating the oversight of AI embedded in very large online platforms and search engines at Commission level by assigning this oversight to the AI Office.

Extending measures in support compliance:

- Allowing providers and deployers to process special categories of personal data for ensuring bias detection and correction, subject to appropriate safeguards;
- Broadening the use of AI regulatory sandboxes and real-world testing so more innovators can benefit from these tools. This includes setting up an EU-level regulatory sandbox from 2028 to support real-world testing.

Improving the AI Act's procedures and operation:

- Clarifying the interplay between the AI Act and other EU laws. Simplifying procedures to foster the timely availability of conformity assessment bodies.

How will these proposals benefit businesses?

According to the Commission's first estimations, the proposed measures on AI are expected to reduce compliance costs for businesses throughout the EU.

At the same time, by extending benefits granted to SMEs to include SMCs, the Commission is making implementation easier for an additional 8,250 companies in Europe.

Overall, the proposals presented today will help businesses meet their obligations. They also open up more opportunities to innovate in the EU, further facilitating the roll-out of the regulatory framework that is designed to create a single market for trustworthy AI.

What are the new timelines proposed?

The proposal acknowledges the challenge that the delay of standards and other support tools cause for the implementation of the AI Act.

The timeline for the high-risk AI rules is aligned to the availability of standards and other support tools. Once the Commission confirms these are sufficiently available, the rules will start to apply after a transition period.

This flexibility has an end date: the rules for high-risk AI in sensitive areas like employment and law enforcement (Annex III) will in any case apply maximum 16 months later than originally envisaged, the rules for high-risk AI embedded in products like medical devices (Annex I) will apply a maximum 12 months later.

The proposal also suggests a transition period of 6 months for providers who need to retroactively include technical solutions into their generative AI systems to make them detectable. For AI systems that are newly placed on the market, the 6 months of application of the rules is a grace period during which no penalties can be imposed.

4. The Data Union Strategy

What is the Data Union Strategy?

The Strategy proposes measures that unlock data for AI across Europe, ensuring that the businesses in the EU have access to high-quality data to compete in the global markets and drive innovation. This will, in particular, help optimise healthcare, improve energy systems and sustain our industrial leadership.

It is centred around **three areas of action** to turn rules into results:

1. **Scaling up access to data for AI**, with initiatives such as data labs, a strengthened focus on the development of Common European Data Spaces (https://digital-strategy.ec.europa.eu/en/policies/data-spaces), including on defence, and developing synthetic data in areas where real-world data is scarce.
2. **Streamlining data rules**, making sharing data easier while protecting rights. Complementing the simplification proposals in the omnibus the Commission will produce further guidance and templates to help companies comply with data rules and introduce a Data Act legal helpdesk.
3. **Strengthening the EU's global position on international data flows**, to ensure fair cross-border data flows while maintaining safeguards for EU sensitive non-personal data and boosting the EU's voice in global data governance. This will complement the long-lasting EU approach to safe personal data flows developed through the EU data protection acquis.

How will data labs work?

Data labs are specialised facilities designed to give companies, including small and medium enterprises (SMEs) and researchers access to diverse datasets for AI. They will provide hands-on services to help organisations share and use data safely.

For example, if a company wants to develop an AI system for a particular area, but struggles to get enough high-quality data, data labs integrated into AI factories will help them overcome this barrier.

Through a data lab, the company would be able to access trusted datasets from the relevant data space, public operators and participating companies – bridging the gap between data spaces and the AI ecosystem so SMEs can train robust AI models while companies' confidentiality is safeguarded.

5. The EU Business Wallets

What are the Business Wallets?

The European Business Wallets are digital tools that will make it easier for companies of all sizes to interact and communicate securely with public authorities and other businesses anywhere in the EU.

The tool reduces administrative burden by allowing businesses to prove their identity, sign and send official documents, or share licences and certificates digitally, with full legal value. The use of business wallets will transform potential obstacles into opportunities for growth and competitiveness. This flagship single market initiative represents a big shift for businesses.

When will the Business Wallets be available?

According to the Commission's proposal, all levels of public administration across the EU, including EU institutions, bodies and agencies, will have two years to implement the use of the business wallets with transitory measures for leveraging existing similar systems at Member State level.

In parallel, the Commission will work closely with Member States and the private sector to define the technical standards and requirements for European business wallets through ongoing efforts under the European Digital Identity Framework (https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation) and in large-scale pilot projects funded under the Digital Europe Programme (https://digital-strategy.ec.europa.eu/en/activities/digital-programme) such as the WeBuild consortium (https://www.webuildconsortium.eu/).

Will companies and public bodies be obliged to use them?

Companies will not be obliged to use the European business wallets. The Regulation places obligations solely on public sector bodies to accept its core functions, while companies remain free to decide whether to adopt the wallets for their commercial operations or interactions with public authorities.
