Briefing on the leaked EU Digital Omnibus proposals

13 November 2025

The changes reportedly being considered in the Data and AI Omnibus proposals – targeting the GDPR, ePrivacy Directive and AI Act – raise serious concerns whether people will enjoy meaningful safeguards around privacy and wider AI risks, whether they will be to fairly access the job market in an environment dominated by AI and automated decision making, and whether they maintain choice and agency over how their health data is processed.

As it stands, **the Omnibus would be the most significant and extraordinary retrenchment in digital rights in a generation – fundamentally altering the presumption that control of people's data should be their own and that they should have choices in how they are subject to AI.**

The impact would be severe - not purely on people - but on the shape and character of the future EU AI market, incentivising 'race to the bottom' compliance behaviours, punishing companies pursuing responsible AI, and challenging the push for greater European sovereignty. Where the Omnibus's narrative claims to prioritise European companies (and especially SMEs), the benefit of the proposals themselves would clearly accrue to existing digital market incumbents.

Please find below a **bullet point synthesis** of the real impact the proposals will have, if materialised, on people's everyday life, access to jobs and skills, health and on European small and medium enterprises.

If the proposals materialise, the real-world impact on people's everyday life, rights and protections would be:

- **Legitimising mass non-consensual data brokerage**
  - Through the **revised definition of 'personal data'** it will become much easier for companies to build up profiles of people and share them without any regulatory scrutiny, as long as the persons are represented through 'pseudonyms' or user IDs and the data controller does not have the direct means to link that pseudonym back to a natural person.

- **Example:** A data broker collects browsing histories linked to device IDs from various apps and websites with location data and purchase patterns under the same ID. If they do not have a 'means reasonably likely' to re-identify the people in the dataset, they can sell this detailed behavioural dataset to insurance companies or political campaigns. The data broker will not have to consider if those getting access to the data have the means to re-identify the people in the data set, they don't need to have any regard for potential risks or regulatory scrutiny.

- **Removing protections from sensitive inferences**
  - **Changes to 'sensitive data'** would no longer cover information that reveals sensitive information, leaving the door open for personalised content, profiling and political advertising based on inferences about people's health, sexual orientation and online preferences and behaviour.
  - **Reality:** Most of the time, data about people's sensitive characteristics are derived from correlations between data points. For example, differences in shopping preferences might indicate that someone is pregnant (even if they themselves are not yet aware), location data can reveal whether a person is in a gay bar or at a hospital. The frequenting of certain webpages might indicate someone's political party affiliation, even if they have not publicly declared their political preferences on their online profiles.
  - **Example in work context:** A courier company tracks employee work phone locations and notices regular visits to a health clinic during lunchtime breaks. The company infers a health condition about the employee which was not explicitly disclosed. Under the revised provisions, the sensitive information inferred from location data would lose special protection and the employer would be able to keep it 'on record' for decisions about promotions, task assignments or potential layoffs.

- **Legalising today's unlawful AI training practices**
  - **Legal basis for AI training.** The introduction of legitimate interests as legal basis for processing personal data for AI training and development inadvertently recognising that today's legal practices are unlawful. Instead of changing the technology, the European Commission's approach is to bend the law to accommodate it.
  - **Reality:** Most commercially offered LLM-based systems have been built through mass scraping of the internet and resultant ingestion of personal data without consent. Developers have tried claiming legitimate interests as a lawful basis for this processing, ignoring people's expectations, choices and concerns. For example, **only 7% of users in Germany want Meta to use their personal data for AI.**

Ada Lovelace Institute
100 St John Street
Farringdon, EC1M 4EH

adalovelaceinstitute.org
hello@adalovelaceinstitute.org
+44 (0)20 7631 0566

Part of the Nuffield Foundation
Registered charity: 206601

- Fueling AI at the expense of people's rights and protections
  - **Modifications to rules around 'sensitive data'** would allow processing of special category data for AI training if there is a 'disproportionate effect' from the data controller to remove sensitive information. It will be at the discretion of AI developers to set the limit for what is responsible processing, turning an important protection for special category data into a convenience exercise – 'what level of effort am I as a developer ready to technically or financially invest?'. The measure would disincentivise the development of privacy-preserving research by developers (for example, 'machine unlearning') because once technically feasible, DPAs would expect developers to use such measures.
  - Further changes include a new **derogation 'for residual processing'** of sensitive data for AI development (subject to certain conditions).
  - **Reality:** This makes it legal for AI companies to scrape data from the internet including highly sensitive personal details and use it for AI training purposes, but also to process any data in the course of operation of an AI system.
  - **Example:** The information that a user shares with their chatbot could be re-used to train an AI model based on this ground even if the user has not consented to this. Once sensitive data is in a model and it would require a 'disproportionate' effort on the AI company to remove the data from the model, then the company does not need to remove such data. **This flips the proportionality test upside down: instead of the rights of the individual guiding when processing is proportionate, it is instead focused on what effort of the AI company is proportionate.**

- Legitimising automated decision-making without consent or public interest
  - **Modifications to automated decision making** shift the framing from a prohibition to cases where ADM is permissible. Where automated decision making is necessary for the performance or for entering into a contract, the controller will have full discretion whether to use automated decision making. In practice, this will lead to vastly more usage of automated decision making while risks and harms are not mitigated.
  - **Example:** A supermarket chain operates an automated system to allocate shifts to warehouse workers and set variable levels of pay. It uses AI to analyse productivity of individual workers to automate task placements and to determine contract termination. The system is also used to make inferences about the potential performance of prospective employees as part of the pre-hire sifting process, leading to potential automated rejections, discrimination and unfair practices.

Ada Lovelace Institute
100 St John Street
Farringdon, EC1M 4EH

adalovelaceinstitute.org
hello@adalovelaceinstitute.org
+44 (0)20 7631 0566

Part of the Nuffield Foundation
Registered charity: 206601

- **ePrivacy rules on terminal equipment moved to the GDPR to expand the lawful grounds**
  - The proposal intends to **move the legal regime for processing personal data on terminal devices** from the ePrivacy Directive to the GDPR. It introduces and exception to cover the specific purposes for processing personal data on terminal equipment which do not require a lawful ground.
  - **This is unprecedented.** GDPR is built on the basis that for any processing of personal data there needs to be a lawful ground.
  - **Key consequence** of this is that **non-personal data will enjoy the much stricter protections** under the ePrivacy Directive.
  - **Example:** Websites claim extensive user tracking – recording every click, scroll, hover and time spent – falls under 'audience measurement' for their own purposes. They interpret this exception broadly to include building behavioural profiles, A/B testing and measuring emotional responses to ads through engagement patterns without consent or any assessment. The collected data reveal user's vulnerabilities (financial struggles, health conditions, addictions), effectively turning the measurement exception into a backdoor for comprehensive behavioural surveillance and monetisation by large technology companies.

- **Europe's sovereignty**
  - Jurisdictions around the world modelled and implemented their data protection regime after the EU (often times verbatim). **If the proposals materialise, the EU will effectively offer much lower levels of protection, deeply damaging its position as a digital leader, weakening its leverage and putting its sovereignty at stake** by enabling other states to take advantage of the resulting vacuum.
  - The proposed changes are likely to advantage large, often foreign-based AI companies, whilst failing to deliver the simplification or support that could realistically benefit European SMEs. With this proposal, **the European Commission is making trade-offs that skew in favour of foreign multinationals**, whilst trading away protections against foreign interference and exploitation of individual vulnerabilities by foreign and private actors. Such trade-offs are unlikely to strengthen the EU's global position or sovereignty in the long run.

- **Societal and democratic resilience**
  - **The scale of the proposed changes requires robust evidence and the publication of a full fundamental rights impact assessment,** evaluating the removal of safeguards as a whole, instead of one by one. The proposed changes are deeply unsuitable for a fast-

Ada Lovelace Institute
100 St John Street
Farringdon, EC1M 4EH

adalovelaceinstitute.org
hello@adalovelaceinstitute.org
+44 (0)20 7631 0566

Part of the Nuffield Foundation
Registered charity: 206601

track omnibus procedure, especially considering that the proposed changes create vulnerabilities for individuals and European democracy.

- **Reality:** The proposed changes on the definition of 'sensitive data' allow for data on inferred political orientation to be processed where previously more stringent protections were in place. This would **enable political targeting of individuals that could negatively impact on democratic norms throughout Europe.**
- **Example:** A social media company could bundle data on a group of users (for example, users of a certain nationality, or living in a certain region). This data could include their likes and visits to certain profiles that does not *directly* reveal the user's political orientation, but from which their political beliefs can be inferred from with relative ease. If the dataset is then pseudonymised to only refer to 'advertising profile of User123', under the proposed GDPR changes, the company could sell and share the dataset legally with other actors. A foreign actor might buy up a dataset of users in a country with upcoming elections, use an AI system to find correlations between the data points to infer political beliefs, and target users accordingly with advertising or information to push them in a certain political direction.

- Businesses
  - SMEs have spent seven years building compliance technology and talent for the current regime – to claim proposals that would result in such fundamental reconfiguration of the regime would benefit SMEs is disingenuous, contradicting the evidence received by the Commission
  - SMEs asked for 'tailor-made support, such as templates and checklists' and for more practical guidance and engagement from data protection authorities.
  - Whereas organisations today look for services which comply with EU's high privacy and security standards, these changes will mean they look elsewhere for markets and service providers able to meet their needs
  - The introduction of broad subjectivity throughout the compliance process is precisely the kind of legal ambiguity that leaves SMEs inhibited from moving fast, and (non-EU) incumbents with large legal teams and risk appetites able to take advantage and further concentrate their market power.

Ada Lovelace Institute
100 St John Street
Farringdon, EC1M 4EH

adalovelaceinstitute.org
hello@adalovelaceinstitute.org
+44 (0)20 7631 0566

Part of the Nuffield Foundation
Registered charity: 206601