Why the Digital Omnibus puts GDPR and ePrivacy at risk

A fast track on rules that safeguard daily life

On November 19, the Commission will present a "Digital Omnibus" package, a series of measures to allegedly ease administrative burdens for businesses across areas like privacy, cybersecurity and artificial intelligence. This will include one proposal dedicated to the AI Act, and another to simplifying digital rules, reopening and amending both the **General Data Protection Regulation (GDPR)** and the **ePrivacy Directive**.

A few so-called **'reality-check' meetings have been held with selected stakeholders** and a **Call for Evidence has been issued** under the Simplification Agenda. Notably, however, the call does not mention any amendments to the GDPR. Yet, **a fundamental-rights impact assessment is lacking**, as is a clear demonstration of necessity and credible evidence that reopening these laws would increase legal certainty.

As part of the broader deregulatory agenda that has already targeted the GDPR through **the Fourth Omnibus on the EU Single Market**, the Commission's proposed 'simplification' would, in practice, **rewrite the meaning of consent, transparency, and device-level privacy across the Union**. These changes would **erode people's ability to control their personal information and to communicate privately**, rights anchored in the EU Charter and inseparable from others like freedom of expression and non-discrimination.

1. Definition of personal data (GDPR Article 4)

What changes

Protection would depend on **whether each organisation claims it can identify a person**, rather than on whether the information is about an identifiable individual in general. While the aim is supposedly to align the GDPR with the SRB European Court of Justice (CJEU) ruling, in practice **this would turn the objective definition of personal data into a controller-specific one**. This would allow companies argue that information is 'non-personal' simply because they claim to lack the means or intent to identify someone, even when others could easily do so.

Authored by Itxaso Domínguez de Olazábal

The draft also **allows the Commission define anonymisation standards through secondary legislation**. That would effectively unable future executives to redraw the GDPR's boundaries without scrutiny from the Parliament or the Council , creating inconsistencies across the AI Act and Data Governance Act.

Why it matters

It **turns a clear, universal rule into a subjective one**. Companies could decide that data are 'non-personal' and process them without safeguards. That would strip people of basic rights such as access, correction, and deletion, and make data protection dependent on corporate interpretation.

A practical example

In 2010, Google admitted that its Street View cars had collected fragments of personal data - including emails and browsing information - from unencrypted Wi-Fi networks while mapping streets. Initially, **the company i claimed the data were anonymous technical information,** but investigations showed they contained personal communications from identifiable individuals. This incident highlights the importance of objectively defining personal data: whether or not Google intended to identify people was irrelevant, because the data related to identifiable individuals. A subjective definition, like the one proposed in the Omnibus, **would risk reclassifying such information as 'non-personal' and remove it from legal protection altogether.**

2. Special-category data (GDPR Article 9)

What changes

Only data that directly reveals health, political opinions, religion, or sexuality would count as 'special category data. Inferred information would no longer receive extra protection.

Why it matters

Modern discrimination happens through inference. Algorithms can guess pregnancy, illness, or political beliefs from behaviour patterns, and act on those guesses. Removing protection for inferred traits means removing protection where bias is most likely to occur.

A practical example

In 2024, the Court of Justice of the EU ruled in the *Lindenapotheke case* that information entered by customers when ordering pharmacy-only medicines online counts as health data, even when the medicines are non-prescription. The Court clarified that, if the data allow conclusions to be drawn about a person's health status, it is to be considered as sensitive under Article 9 GDPR, regardless itsaccuracy or whether the purchase was made on behalf of someone else. The judgment confirms that health data protection extends to seemingly ordinary transactions. **Weakening this rule, as the Commission seemingly proposes, would ignore the CJEU's reasoning and legitimise processing practices that can expose people's vulnerabilities.**

3. A new 'legitimate interest' for AI development and operation (GDPR Articles 9(2)(k) and 88c)

What changes

Training and operating AI systems would be allowed under **legitimate interest, a legal basis meant for limited cases where a controller's need to process data is balanced against people's rights**. It normally applies to low-risk situations, such as preventing fraud or ensuring network security, rather than large-scale data use. Extending it to AI would mean that companies could collect and reuse personal information without asking for consent or demonstrating a specific need.

Why it matters

Your posts, photos, and voice recordings could be repurposed to train commercial AI models without your permission. Once data are built into a model, removing them is practically impossible. **This normalises surveillance-based innovation and rewards the biggest data holders**. The reasoning behind the new recital **confuses necessity with legality**: because AI systems need vast data to function, the draft assumes that processing must therefore be lawful. That flips the interpreation of Article 6(1)(f) on its head and even conflicts with the Digital Markets Act, which forbids gatekeepers from merging personal data across services without consent.

A practical example

Seven lawsuits have recently been filed in California alleging that OpenAI's ChatGPT had caused psychological harm and even suicide by providing manipulative or dangerous advice. The controversy underscores what happens when powerful AI systems are trained and deployed without effective oversight or clear accountability. **Granting companies a blanket legitimate interest to train such systems would make that kind of unaccountable processing the norm rather than the exception.**

4. Transparency duties (GDPR Article 13)

What changes

Controllers would be **exempt from full information duties** if they believe the relationship with the user is 'clear and circumscribed' or if they think the person 'already has' the information.

Why it matters

Transparency would become optional. **People would no longer be clearly informed about what data is collected, for what purpose, or for how long it is kept for**. Without this knowledge, rights like access, objection, or erasure lose all meaning.

A practical example

In 2025, the Irish privacy watchdog fined TikTok €530 million for,, failing to meet its transparency obligations regarding transfers of European people's data to China, among other infringements. TikTok's privacy policy did not list all third countries to which data was transferred, nor did explain that Chinese-based staff accessed information stored elsewhere. Only after the

investigation, TikTok updated its privacy policy to comply. **This case shows how even large platforms struggle to meet basic transparency duties, and why relaxing these obligations would allow opaque practices to continue unchecked.**

5. Access rights and motive tests (GDPR Articles 12(5) and 15)

What changes

Organisations could refuse access to personal data if they suspect the request is not made for data-protection purposes or is 'exploitative.'

Why it matters

This would **make rights conditional on motives**. People often use access rights to uncover unfair or discriminatory practices. **Allowing companies to question intentions would reverse accountability and deter legitimate oversight.**

A practical example

A digital rights organisation investigates how a major social-media company tracks people across websites. To document the practice, users file access requests to see what browsing data the platform holds. However, the company refuses, claiming the requests are 'not for data-protection purposes' but part of an advocacy campaign. Without access, the organisation cannot prove the scale of tracking or submit a well-founded complaint to data-protection authorities.

6. Breach notification and the single entry point (GDPR Article 33)

What changes

Only breaches posing a 'high risk' would need to be reported. The deadline would be extended from 72 to 96 hours, and notifications would pass through a central EU portal before reaching national authorities.

Why it matters

Most breaches would never reach data-protection authorities, meaning patterns of poor security would go unnoticed. **People could wait weeks to find out that their data had been exposed, reducing their ability to prevent fraud or identity theft.** Routing all notices through a central portal run by a cybersecurity agency, rather than data-protection authorities, risks delays and weakens independent oversight.

A practical example

The UK Ministry of Defence has suffered at least 49 separate data breaches in the Afghan relocation scheme over the last years. One of them exposed the personal details of nearly 19,000 Afghans who had worked with British forces and were seeking refuge. The government initially tried to keep the incident secret under a court order, and victims learned of it only months later. Lawyers described the pattern as "catastrophic failings", with repeated leaks despite earlier promises of reform. This case shows the **human consequences of weak reporting obligations: when disclosure is delayed or filtered, those affected lose the chance to protect themselves, and institutions escape real scrutiny**.

7. ePrivacy folded into the GDPR: device access and communications confidentiality

What changes

The proposal would incorporate ePrivacy's consent rule into the GDPR. Instead of requiring your prior agreement before information is stored or read on your devices (e.g. cookies, apps, connected devices), **companies could rely on legitimate interest or vague grounds such as 'security' or 'audience measurement.'**

Why it matters

Consent is a clear, user-driven safeguard: **nothing happens on your phone, computer or smart device unless you agree.** Legitimate interest reverses that logic. It allows companies to decide for themselves that their commercial or technical goals outweigh your right to privacy. **Accessing your device or monitoring your communications would no longer be an exception, it would become routine.**

A practical example

The Databroker Files investigation by netzpolitik.org, Le Monde, and L'Echo uncovered a vast trade in location data from smartphones showed that adtech tracking - nominally done for 'audience measurement' - has turned into a surveillance infrastructure. **Weakening ePrivacy to allow such practices under legitimate interest would legalise precisely the kind of opaque data trade that already threatens people's safety and the confidentiality of communications.**

8. Privacy signals: the good news - with caveats

What changes

The proposal also introduces a new Article 88b on **Privacy Signals.** These would allow browsers or devices to **automatically communicate whether people consent or not to be tracked,** replacing the need to click through endless pop-ups. However, the system would only take effect after new technical standards are developed, and media service providers would not be required from having to respect these signals.

Why it matters

Privacy Signals could finally make consent meaningful and reduce manipulation, but **the long delay and the media exemption risk turning them into a symbolic gesture.** In practice, the very websites that rely most on advertising could keep tracking readers, undermining trust in journalism and perpetuating surveillance advertising models.

A practical example

A person configures their browser to refuse tracking. This setting works on some platforms, but when they read a news site, the page still loads dozens of third-party trackers or forces you into a 'Pay or Okay' paywall. The site claims it's a media provider and, as such, is not obliged to honour the signal. What should have been a simple privacy tool ends up reinforcing the very system it was meant to challenge.

Deregulation disguised as reform and what next

Each drafted amendment moves us further away from enforceable rights toward corporate discretion. Together, they would make people less able to know, contest, or prevent how their information and communications are used.
The reforms also fail on their own stated goal: **they would not provide legal certainty**. Redefining key terms and fragmenting enforcement would make compliance less predictable, not more. **There is no evidence that weakening the GDPR and ePrivacy would enhance EU competitiveness, but clear evidence that it would erode trust.**

The Commission still has time to change course before the Digital Omnibus is formally proposed on 19 November. It should **withdraw its plans to reopen the GDPR and ePrivacy frameworks** and focus on enforcing and improving the laws that already work.

Real simplification does not come from rewriting rights but from making compliance clearer and enforcement stronger. The Commission should:

- prioritise the consistent application of the GDPR and ePrivacy regulations across Member States;
- support and resource data-protection authorities and other regulators to enable them to act effectively and in coordination; and
- ensure that Privacy Signals become interoperable, immediate, and binding from the start, without carve-outs that would weaken them.

Europe's credibility as a defender of digital rights depends on upholding the protections it built, rather than reopening them under pressure to deregulate.