Why the Digital Omnibus puts GDPR and ePrivacy at risk

A fast track on rules that safeguard daily life

On November 19, the Commission presented a "Digital Omnibus" package, comprising a series of measures to allegedly ease administrative burdens for businesses across areas such as privacy, cybersecurity and artificial intelligence. As planned, this included one proposal dedicated to the AI Act, and another to simplifying digital rules, reopening and amending, amongst other data-related rules, both the **General Data Protection Regulation (GDPR)** and the **ePrivacy Directive**.

A few 'reality-check' meetings were held with selected stakeholders and a Call for Evidence was issued under the Simplification Agenda. The call did not mention any plan to amend the GDPR. Nevertheless, **the Commission moved ahead with a proposal that reshapes core protections without conducting a fundamental-rights impact assessment.** The Digital Omnibus include a short section claiming to address fundamental rights, but it focuses almost entirely on the supposed 'right to conduct a business,' which is not a fundamental right in itself. Furthermore, it does not explain how the changes would preserve the highest level of data protection nor how people's rights would remain safe once key safeguards are weakened.

The Commission's simplification is part of the broader deregulatory agenda, which we have condemned with over 470 civil society groups and trade unions. This agenda has already targeted the GDPR through the Fourth Omnibus on EU Single Market, **rewriting 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.** These rights are anchored in the EU Charter and are inseparable from other rights, like freedom of expression and non-discrimination.

This piece builds on an earlier explainer of the leaked draft. The final proposal is now public. It is followed by a call for evidence, and a full legislative procedure with EU Member States and the European Parliament , despite clear signs of political pressure and limited democratic scrutiny. The proposal comes at a moment of political pressure from different sources – including European governments and Big Tech - to weaken digital rules in the name of competitiveness. Yet, there is no clear evidence that these changes would make the law easier to follow or, even worse, safer for people.

1. Definition of personal data (GDPR Article 4)

What changes

Today, information counts as personal data if it could reasonably be used to identify a person. The proposal weakens this rule. **Organisations would be allowed to say that some information is not personal data if they claim they cannot identify anyone from it, even if others could.** This matters for data that today fall under the GDPR because they are only pseudonymised, not anonymous. The proposal also gives the Commission new powers to decide when certain types of pseudonymised data should be treated as non-personal.

Why it matters

It **turns a clear, universal rule into a subjective one**. This means that the status of data depend on what each organisation decides. Two companies holding the same information might treat it differently. If an organisation classifies data as 'non-personal,' then people lose the rights they currently have over that information.

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 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.**

A supermarket loyalty programme tracks every purchase linked to a customer ID. Today this is personal data because the patterns reveal who the customer is. Under the proposal, the supermarket could claim these records are 'non-personal' since it does not identify anyone itself, allowing the detailed purchase history to be shared with insurers or advertisers without people knowing or being able to object.

2. Special-category data (GDPR Article 9)

What changes

Sensitive data are pieces of information that reveal or strongly suggest details such as a person's health, sexuality, political opinions, religious beliefs, or biometric details used to identify them. This type of data receive the strongest protection in EU law because its misuse can cause serious harm.

The proposal keeps the definition, but creates several new routes for sensitive data to move into AI systems. One new rule allows sensitive data to stay in AI training datasets if its removal is considered too difficult. Another allows companies to use biometric data for identity checks when they say the information stays 'under the person's control.' The Omnibus proposal also amends the AI Act. A new Article 4a permits companies to process sensitive data to detect or correct bias in AI systems, even when the system is not high-risk.

Why it matters

These changes make it far easier for sensitive information to circulate inside AI models. Companies gain multiple ways to use or keep sensitive data, even when people never consented or expected this. The new bias-correction rule in the AI Act adds an extra doorway for sensitive traits to be processed. The result is weaker protection in practice, especially when sensitive attributes support profiling or influence decisions.

A practical example

In 2021, the Norwegian Data Protection Authority fined Grindr for sharing data with advertisers that revealed users' sexual orientation, simply because they were using the app. The authority held that this was sensitive data, even though users had not explicitly stated anything about their sexuality. Under today's rules, this information receives the highest level of protection. Under the proposal, data of this kind could slip more easily into AI systems. Companies would be able to keep such sensitive signals in training datasets if they argue that removing them is too difficult, or process them for 'bias correction' under the AI Act. This would create new paths for sensitive traits to be reused in ways people neither agree nor control.

A taxi app logs late-night trips to LGBTQ+ venues or clinics. Today, this is treated as sensitive data because it reveals aspects of a person's identity. Under the proposal, these signals could remain inside AI training datasets if a company argues that removing them is too difficult, exposing people to profiling they cannot see or influence.

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

What changes

Under current law, companies need a strong and specific reason to reuse people's data to train AI systems and even stricter safeguards are required for sensitive data . The proposal changes this. **It allows companies to rely on 'legitimate interest' for AI training.** This is a flexible ground that companies define for themselves, not something people agree to. It gives organisations wide freedom unless a person objects, and most people are unaware when their data is used in this way. The proposal also says sensitive data may stay in training datasets if removing them is considered too hard. On top of this, it expands the definition of 'scientific research' to include commercial product . This weakened definition makes it easier for companies to treat almost any AI project as compatible with the original purpose for which the data were collected.

Why it matters

These changes make large-scale reuse of personal and sensitive data far easier. Companies will be able to treat commercial AI development as research and reuse data on that basis. The proposal creates a right to object to AI-related processing, but this right is difficult to exercise as people have no way to know which training datasets contain their data.

A practical example

Seven lawsuits have recently been filed in California alleging that OpenAI's ChatGPT had caused psychological harm, including 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' pass to train such systems would normalise unaccountable processing**

A language-learning app stores thousands of short voice clips from users. Today, reusing these recordings to train a commercial speech-recognition model requires a clear legal basis and proper notice. Under the proposal, **the company could label this as 'legitimate interest' and 'research,' reusing people's biometric voice patterns without telling** them or offering a meaningful chance to object.

4. Transparency duties (GDPR Article 13)

What changes

Today, organisations must give people clear information about what they collect, why they collect it, and how long they keep it. **The proposal allows companies to skip detailed explanations if they believe the person already knows what is happening, or if they consider the relationship as 'clear' enough.** In research contexts, companies can publish generic statements instead of notifying individuals directly.

Why it matters

Transparency would become optional. **These changes would make it easier for organisations to explain less.** Without clear information, people struggle to understand or challenge what happens to their data. This weakens the effectiveness of every other right in the GDPR.

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.**

A food-delivery platform starts analysing riders' phone-sensor data to estimate speed and 'efficiency.' Instead of alerting riders, the company says the change is obvious from the nature of the job and updates a generic privacy page. Riders continue working without knowing that new metrics are shaping their profile and affecting their opportunities.

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

What changes

Today, anyone can ask for a copy of their personal data without giving a reason. However, the proposal introduces 'motive tests,' **allowing companies to refuse access if they suspect the request has the wrong purpose or is part of a dispute.** Companies may also claim that the person already knows the relevant information.

Why it matters

This would **make rights conditional on motives**. Access rights help uncover misuse, discrimination, and errors. Allowing companies to question motives discourages people from exercising this right and allows organisations to block investigations that rely on access requests.

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** for further investigation to data-protection authorities.

Warehouse workers ask for the data used by the system that assigns shifts. The employer refuses, saying the request is part of a labour dispute rather than a data-protection right. **Without access, the workers cannot check whether the system is fair** or whether mistakes are costing them income.

6. Automated decision-making (GDPR Article 22)

What changes

Today, the GDPR limits important decisions that are made entirely by automated systems. A human must be involved, unless specific conditions apply. The proposal removes this limit. **Automated decisions could become broadly allowed whenever a company considers them necessary for a contract or a service.**

Why it matters

This makes it easier for companies to rely on automated systems in areas such as hiring, credit scoring, insurance pricing, or content moderation. People may receive important decisions from systems that are hard to challenge and that lack meaningful review.

A practical example

The *SCHUFA* case showed why limits on automated decisions matter. **Germany's credit-scoring agency used automated profiling to decide whether someone was creditworthy.** People had little insight into the factors behind their score and limited ways to challenge errors. The CJEU confirmed that such decisions fall under Article 22. Under the proposal, systems like this would become easier to justify as 'necessary for a service,' leaving people more exposed to opaque credit decisions.

A rental platform uses an automated scoring system that screens applicants based on online traces and neighbourhood data. People with lower scores are rejected instantly without being able to speak to a person. Under the proposal, the platform could classify this as 'necessary for the service,' making such opaque decisions harder to contest and easier to justify.

7. Device access and communications confidentiality (ePrivacy Directive Article 5.3)

What changes

Today, ePrivacy requires sites and apps to obtain your consent before storing or reading information on your device. This applies to all data, whether personal or not. **The proposal keeps ePrivacy but turns off this consent rule whenever the access involves personal data.** A new GDPR article takes over instead. Under this new rule, companies can access data on a device in three ways: 1) with consent, 2)under EU or national law for public-interest reasons, or 3) through four broad exceptions that cover communications, providing a requested service, first-party audience measurement, and security**.** When access falls inside one of these exceptions, companies do not need a separate legal basis to continue using the data for the same purpose.

Why it matters

This changes a simple rule into a **more permissive system.** Consent has been the backbone of device privacy. Replacing it with a mix of broad exceptions gives companies far more room to track behaviour, measure usage, or analyse interactions directly on people's devices. **It also weakens the long-standing protection that kept digital communications confidential, because many activities that used to require consent will no longer need it.**

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 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.**

A messaging app reads device information to estimate how quickly messages appear on screen and which notifications are opened. Today, this requires consent. Under the proposal, **the app could use the 'security' exception to read and store these signals without permission**, making people's communication patterns available for analysis without their knowledge.

8. Privacy signals: the good news - with caveats

What changes

Today, browser or device-level signals that express consent or refusal are not legally binding. **The proposal introduces privacy signals as a standard way for people to refuse tracking. Companies must respect these signals.** But the signal only covers refusal. Acceptance still requires a pop-up. Media outlets are not required to honour the refusal signal.

Why it matters

Privacy signals would make refusal simpler and clearer. They are mandatory from the start, which is a positive step. **But their effectiveness is limited by a major exception for media outlets.** These providers are not required to respect the refusal signal and can still present their own consent requests. This means people will continue to face banners on many

news sites, even when their browser or device has already sent a clear refusal. The result is an uneven experience and weaker protection where much of the tracking pressure comes from.

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.**

9. Why the Digital Omnibus matters for policing and state surveillance

What changes

Recital 41 quietly extends all GDPR amendments in the Digital Omnibus to the Law Enforcement Directive (LED) and the EU Data Protection Regulation (EUDR). While the former regulates data processing by law enforcement competent authorities, the latter governs how EU institutions, bodies and agencies, including Europol and Frontex, collect and use personal data. The Omnibus proposal does not explain this clearly, but the consequence is direct. The narrower definition of personal data, the weaker device-access rules, the new permissions to keep sensitive data inside AI training datasets, and the looser handling of biometric information would not only affect companies. **They would also apply to police forces and other bodies in the criminal justice system.** The level of protection afforded by LED already suffers from insufficient safeguards against state abuse and power. Recital 41 lowers the LED even further to the weakened GDPR baseline.

Why it matters

The timing could not be worse. The European Parliament has just supported a new Europol Regulation as part of the so-called Facilitators Package, expanding Europol's role in the criminalisation of movement. Europol already operates large databases, relies heavily on biometrics and stores vast amounts of personal data for AI training, all with ineffective oversight. EDRi and other civil society organisations warn that these systems disproportionately target racialised and marginalised groups. **Extending the Omnibus' deregulatory changes to policing gives law enforcement agencies broader access to devices, sensitive data, and AI tools at a moment when they are demanding more powers and fewer safeguards**. A technical recital ends up eroding protections where the consequences are most severe.

A practical example

Police stations use facial images to check identities of people brought in for questioning. Today, biometrics use must be strictly limited and justified. Under the proposal, **looser rules on biometric data and a narrower definition of sensitive information would make it easier to store and reuse facial data,** including for training AI systems without people knowing or being able to challenge the reuse.

A wider pattern: deregulation disguised as reform

Each drafted amendment moves us further away from enforceable rights toward greater discretion for those who hold power, whether companies or state bodies. This makes it harder for people to understand, challenge, or stop how their data and communications are used. The sections above explain the so-called 'targeted amendments' one by one, but their combined effect is far more serious. The changes interact: t**ogether, they weaken long-standing safeguards across the digital environment, including in policing and criminal-justice systems.**

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 at a time when both commercial and state surveillance already shape people's lives in far-reaching ways.**

What it should happen next

The Commission adjusted some elements of its approach but kept its plan to reopen the GDPR and ePrivacy rules. It still did not prioritise enforcement and improvement of the existing framework, despite repeated calls from civil society, political groups, and even Member States to do so. **Real simplification does not come from rewriting rights but from making compliance clearer and enforcement stronger.**

Instead, 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.