Corporate Europe Observatory

LOBBY CONTROL

January 2026

Article by article, how Big Tech shaped the EU's roll-back of digital rights

In a new analysis by Corporate Europe Observatory and LobbyControl, we trace Big Tech's fingerprints on the Digital Omnibus proposals - a major deregulation of EU digital laws including the GDPR and the AI Act. They are helped in this attempt by the Trump administration and the European far right.

At the end of November 2025, Ursula von der Leyen gave Trump and his tech oligarchs an early Christmas present: an unprecedented attack on digital rights. In its so-called Digital Omnibus, the European Commission proposed weakening important rules designed to protect us from Big Tech's abuses of power.

These are the protections that keep everyone's data safe, governments and companies accountable, protect people from having artificial intelligence (AI) systems decide their life opportunities, and ultimately keep our societies free from unchecked surveillance.

At the same time, the Digital Omnibus is part of the European Commission's deregulation agenda, which threatens key social and environmental standards in Europe. Ironically this deregulation agenda is being promoted by the Commission as a way to make the EU 'competitive' – despite in reality actively empowering US Big Tech companies that dominate the field.

The Digital Omnibus was immediately heavily criticised by numerous civil society organisations. Politico even called it the end of the 'Brussels effect' – that is, that European tech regulations are adopted in other countries – and wrote that "Washington is [now] setting the pace on deregulation in Europe."

To show the extent of Big Tech's influence on the Digital Omnibus, we compared the Commission's proposals with the lobbying positions from Big Tech and its associations. v

The proposals in the Digital Omnibus concern both data protection and rules for AI. While the EU mistakenly speaks of benefits for European corporations, it is clear that weak digital rules strengthen the power of Google, Microsoft, Meta etc, thereby jeopardising the goal of becoming more independent from Big Tech and the US.

In the past, Big Tech has repeatedly spread the one-sided lobbying message that data protection hinders economic growth and innovation, especially with regard to AI. This includes exceptions for SMEs and a fundamental focus on making more use of data instead of protecting it.

Tech companies are spreading these messages with a record-breaking lobbying budget, a huge lobbying network, and support from the Trump administration. The digital industry's annual lobby spending has grown from €113 million in 2023 to €151 million today – an increase of 33.6 percent in just two years.

Now, the European Commission appears to be bowing to this lobbying pressure and adopting key lobbying messages from Google, Microsoft, Meta and their many lobby organisations in its Digital Omnibus.

Here we break down these industry lobbying messages, how they have been adopted by the Commission as proposed text changes, and what the real world impacts could be.

How the Commission aims to weaken the GDPR and ePrivacy

The General Data Protection Regulation (GDPR) is the backbone of the EU's digital rulebook. While the Commission claims it is only giving the GDPR a "face-lift", its proposed changes - from the definition of personal data to the use of data for training AI - will have far-reaching consequences to people's rights, and will benefit Big Tech's problematic business model based on massive data extraction.

Limiting the definition of personal data

The Commission intends to stop classifying pseudonymised data (ie swapping out a user's identifiable name for a code or number) as personal data if a company claims it cannot identify a person, thereby exempting it from GDPR protection. This rule would also apply even when other actors (for instance data brokers) can still identify individuals based on the pseudonymised data.

As the digital rights organisations Noyb and EDRi have pointed out, this change turns a universal rule into a subjective one. GDPR protections will only apply when a company has the means to identify a person based on the data it holds. This gives

huge leeway to companies to decide not to apply the GDPR arguing that they can't identify a person. Worse, data can be sold to other companies or data brokers that do have the means to re-identify individuals.

But even if data is never sold or passed on to third parties, the proposed subjective approach would still severely narrow the scope of the GDPR. Big Tech companies such as Meta and Google for instance could use personal data for online tracking by claiming that the data cannot be traced back to a natural person and is therefore not covered by the GDPR.

Proposed changed text to article 4(1) of the GDPR in the digital omnibus in italics: "Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person.

Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates."

Big Tech's lobby position

This move closely reflects Big Tech's lobby position. The industry has long been calling for greater commercial use of personal data. The use of anonymous and pseudonymous data in particular should contribute to this.

DigitalEurope, (which counts all Big Tech companies among its members), wrote: "Clarify that pseudonymised data is not personal data when recipients cannot reasonably re-identify individuals."

Microsoft Germany also lobbied for weakening the definition along similar lines.

Limiting your right to access your own data

Summary: Currently, anyone can request a copy of their personal data from any company or organisation that holds it. However, the Commission intends to limit this right if a person 'abuses' it.

This will severely limit the rights of individuals to know which of their data is being held by Big Tech. For instance, in 2023 Uber and Ola drivers who were 'robo-fired' won a court case against the company after it refused access to their work-related

information. Ola tried to argue that the drivers requests for data amounted to an abuse of data protection rights, an excuse that the Commission now wants to give a legal basis.

This will make it harder to hold Big Tech to account and to contest their unlawful practices. “The proposal threatens to dismantle a tool of counter-power”, as the academic René Mahieu writes.

Contrary to the claims made by industry, and adopted by the German Government, it is not citizens who have ‘abused’ their right to access their own data, but tech companies that have disregarded this right. According to the privacy organisation NOYB 90 percent of data access requests are not respected. In one case, it took more than five years for Youtube to respect a particular data access request.

Proposed changed text to article 12(5) of the GDPR in the digital omnibus in italics: “Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character *or also, for requests under Article 15 because the data subject abuses the rights conferred by this regulation for purposes other than the protection of their data*, the controller may either: a) charge a reasonable fee [...] or refuse to act on the request.

The controller shall bear the burden of demonstrating *that* the *request is* manifestly unfounded *or that there are reasonable grounds to believe that it is excessive*.”

Big Tech’s lobby position

The German Government lobbied for this change in an influential but controversial position paper. What has largely gone under the radar, however, is that these proposals were actually pushed by Big Tech companies.

In a lobby paper dated 16 August 2025, **Google** called on the German Government to "Introduce a ‘disproportionate efforts’ exemption to compliance with Articles 15-22 GDPR". With regard to Article 12(5), Google proposed the following addition highlighted in bold:

“Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, **or, taking into account the scope of the processing and the cost of implementation, where responding to the request would involve a disproportionate effort**, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request.”

Using your personal data for training AI

Generative AI models are being trained on enormous amounts of data. The Commission intends to permit the training of AI models with personal data, including highly sensitive data such as sexuality, political beliefs, or ethnicity, without active consent. People's data will only be protected from being used for training AI models if they explicitly opt-out.

Tech companies can basically hoover up any personal data on the internet to train their AI models without active consent (opt-out would still be possible). The protection of sensitive data for training AI such as political beliefs, union membership or sexuality is also weakened.

There is a risk of 'data leakage' whereby AI systems reproduce the personal data it has been trained on or produce fake information. In one such case a journalist was falsely accused by a Microsoft chatbot of child abuse when in fact he had just published articles on criminal court cases about it. The AI system, in essence a statistical programme, had conflated this information and had made him out to be a criminal.

Major tech companies such as Meta, Google and X stand to benefit as they can train their AI models with massive troves of personal data collected through their platforms.

Big Tech companies are spending enormous amounts, possibly as much as US$550 billion in 2026, to dominate the AI market. Loosening rules on AI data collection plays directly into their hands.

Proposed text:

- **The digital omnibus introduces a new article 88c in the GDPR introducing the use of personal data for AI training as a legitimate interest**: *"Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f)"*

- **The digital omnibus also waters down protections on using sensitive data for AI training by introducing article 9(5) to the GDPR**: *"For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such*

data. If removal of those data requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties."

Big Tech's lobby position

This has been a top priority of Big Tech lobbying. Almost every trade association and company has lobbied both the Commission and member states on that topic.

Big Tech lobby organisation **CCIA**: "It is crucial to reaffirm the role of legitimate interest as a lawful basis under the GDPR for responsible AI innovation, moving beyond the non-binding EDPB opinion to provide harmonised legal certainty for AI training."

DigitalEurope: "Reinforce the use of 'legitimate interest' as a ground to process personal data for key use cases such as product development – including of AI models – and security."

Big Tech lobby organisation **Dot Europe** (in a lobby letter to the Danish Government): "GDPR Article 9 strictly limits the processing of special category data (e.g., race, ethnicity, health), posing challenges for AI development, particularly in healthcare. AI models need access to sensitive data to ensure accuracy, fairness, and cultural relevance."

Weakening rules on automated decision-making

Currently, automated systems cannot be used to make decisions with legal effect or for online profiling. A human must be in the loop. The Commission's proposal is a structural shift from a general prohibition on automated decision-making but with a few narrow exceptions towards an authorisation regime where a company can employ automated decision-making whenever it thinks this is "necessary".

Important decisions including credit scoring, 'robo-firings', profiling, and welfare benefits could in the future be taken by automated decision-making without human intervention. This change will increasingly expose people to possibly flawed and biased algorithms which could make life-changing decisions, including if you get a loan or are fired from your job. Moreover these algorithms are generally black boxes, meaning it can be hard to uncover evidence of bias. Scandals in the Netherlands and Australia already show how thousands of people can be wrongly targeted with devastating effects.

In 2024, a subsidiary of the food delivery platform Glovo was fined €5 million

by the Italian data protection authority under article 22 of the GDPR for violating workers' rights. The platform had used its rating system to automatically assign orders or ‘deactivate’ (read: ‘fire’) workers based on their ratings.

While the drastic weakening of article 22 will benefit a range of different sectors, from the insurance and banking sector to gig economy companies, Big Tech is also set to profit.

At the moment, social media giants employ thousands of underpaid workers to review harmful or illegal content on social media. This change will allow Big Tech companies to fully automate content moderation, cutting these costs essentially down to zero. Since the inauguration of Trump, Meta has fired thousands of content moderators. Amnesty International has warned that replacing content moderators with automated systems could amplify the most harmful content including content inciting racial hatred.

Proposed text to Article 22 of the GDPR in italics: “*A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision*: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller *regardless of whether the decision could be taken otherwise than by solely automated means*.”

Big Tech’s lobby position

While Big Tech companies have been complaining about the overlap between article 22 of the GDPR with the AI Act and the Platform Work Directive, it seems it was mainly insurance sector lobbying that was decisive in rolling back the protection on automated decision-making (Big Tech is however still set to benefit from this change). In 2023, the European Court of Justice ruled in a landmark case that credit scores based on profiling cannot be used by banks and insurance companies to decide on granting a loan or other financial products. The Digital Omnibus might now undermine that ruling.

Insurance Europe: "Automated-decision making should be allowed as long as it is subject to safeguard mechanisms. To ensure that Art. 22 does not become an obstacle to the development of new digital solutions, it should be clarified that it is a right of the data subject and not an ex-ante prohibition."

Big Tech lobby organisation **CCIA**: “The definitions of the General Data Protection Regulation’s (GDPR) ‘automated individual decision-making’ (Article 22), the AI Act’s

'AI system' (Article 3(1)), and the Platform Work Directive's (PWD) for automated decision-making systems often overlap."

Folding parts of ePrivacy into the GDPR

Cookies are the backbone of the AdTech industry, used to trace our online activities in order to target us with personalised ads. Article 5(3) of the ePrivacy directive requires websites and apps to ask for prior consent before storing cookies. The Commission now wants to 'fold' parts of article 5(3) into the GDPR. This replaces a categorical, consent-based mechanism with a more flexible framework based on balancing and exceptions.

Folding ePrivacy into the GDPR creates a more permissive system that allows companies to use exceptions to track behaviour. The Databroker Files demonstrated that commercial datasets which contain millions of locations could actually be used to spy on the public in Europe. These and other examples show the risks to our privacy are real: reporting shows how the vast trade in location data from smartphones can be traced back to individuals showing where they were at a specific time.

It will allow them to do even more of what they already do: track you without your consent. Big Tech firms have been lobbying for years against ePrivacy as it could undermine their invasive business model based on surveillance ads.

Several Big Tech firms have moreover faced fines for tracking users without consent. This change might let these companies get away with their most problematic practices.

New text added to article 5(3) of the ePrivacy directive in italics: "*This paragraph shall not apply if the subscriber or user is a natural person, and the information stored or accessed constitutes or leads to the processing of personal data."*

A new GDPR article 88a takes over instead which also introduces a series of exceptions to ask for consent including when "creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use".

Big Tech's lobby position

The telecom sector, publishers and the tech industry have lobbied for years against strong privacy protections as guaranteed by the ePrivacy directive. In 2018 a major Big Tech driven lobby campaign prevented efforts to strengthen the ePrivacy Directive. A court document showed Google revealing that "we have been successful

in slowing down and delaying the [ePrivacy Regulation] process and have been working behind the scenes hand in hand with the other companies." The digital omnibus is another step in dismantling ePrivacy protections with all major players pushing for the changes as proposed by the Commission.

Google: "The most effective simplification is to delete Article 5(3) from the ePrivacy directive and govern all data processing related to cookies under the GDPR risk-based framework. Alternatively, a significant step toward simplification would be to amend Article 5(3) to extend the scope of permitted exemptions to allow specific, low-risk processing activities that are essential both for the functioning of a safe and sustainable digital ecosystem as well as for user experience. This would create clear exemptions for functions such as first-party audience measurement, ad frequency capping, and anti-fraud measures—allowing them to operate without generating unnecessary consent requests."

Microsoft: "The "cookie rule" in article 5 (3) eP[rivacy] D[irective] could be moved to the GDPR or, if kept in, rendered more flexible by allowing cookie placement without consent in a wider range of circumstances, e.g. for security, software updates, anti-fraud, and analytics."

How the Commission aims to weaken the AI Act

"Europe is open for AI and for business!" Ursula von der Leyen tweeted during the AI Action Summit in Paris. In its single-minded priority to "win the global AI race", the Commission is slashing rules and protections against risky AI systems. A year-long lobby campaign by the Trump administration and Big Tech to delay the implementation of the AI Act has clearly paid off.

No Checks and Balances for risky AI systems

A controversial win for Big Tech firms during the AI Act negotiations was allowing companies to "self-assess" if they believe an AI system is high-risk. To compensate for that loophole, industry had to register these AI systems in a public database. Now this transparency failsafe will also be removed, basically giving tech companies a free hand in deciding if an AI system is risky without any public oversight.

The risk to fundamental rights these high-risk AI systems pose are far from hypothetical. From algorithmic-powered employee firings to biased algorithms that disadvantage students based on their socio-economic background, highly problematic AI systems are already in circulation. The AI Act lets companies self-assess if these AI systems are high-risk or not, and should therefore comply with requirements such as proper risk management, accuracy, and transparency.

The digital omnibus will worsen an already huge loophole in the AI Act with potentially disastrous impacts on our rights.

Not only can AI companies already self-assess if their AI systems are risky, the digital omnibus will remove any possibility of public oversight of that assessment, giving these companies a blank check to do as they please without any accountability mechanism.

In a reaction on LinkedIn Daniel Leufer from the NGO Access Now called this "the biggest, most ridiculous loophole in the AI Act that will let unscrupulous providers unilaterally exempt themselves from the AI Act's obligations with oversight".

Paragraph 2 of article 49 of the AI Act is deleted.

Big Tech's lobby position

The Commission's proposals are completely in line with the lobby position of the two lobby organisations Dot Europe and DigitalEurope that count Big Tech members as its members.

DigitalEurope: "Abolish the mandatory registration of AI systems, along with the related EU and Member State databases."

Dot Europe: "when a provider of AI systems provides concrete justifications that its AI system does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons per Article 6(3), it should not be required to register its system in the high-risk AI database per Article 49."

Delay in the implementation of the AI Act

The Commission intends to postpone the implementation of part of the AI Regulation by almost a year and a half. This means giving Big Tech more than 12 months to continue releasing potentially risky systems onto the market without any safeguards.

This proposal would enable companies to continue to release risky AI systems for at least a year onto the market without any safeguards. Moreover, as the Center for Democracy and Technology points out, delaying the parts of the AI Act on high-risk AI systems, will also obstruct the ban of the most dangerous AI systems, leaving dangerous practices such as emotion recognition systems and facial recognition AI used in public spaces on the market for longer.

Delaying is a tried and tested industry lobbying tactic. It will give Big Tech more time to further water down the AI Act. Already, tech lobbyists are calling for the further

deregulation of the AI Act.

Big Tech's lobby position

A delay in the implementation of the AI Act is a central demand in a year-long tech lobby campaign which was backed by the Trump administration.

CCIA: "The first priority should be to delay AI Act implementation until at least 12 months after relevant guidance, codes of practice, or technical standards become available."

DigitalEurope: "Delay the application of high-risk AI requirements until at least 12 months after relevant harmonised standards are published, allowing sufficient time for adaptation."

Meta: "It is critical to first pause the implementation and enforcement of the [AI Act]. This pause will provide the necessary time to undertake meaningful reforms without risking the EU falling behind in the global AI race.

Using your sensitive data to train AI

The AI Act under narrow circumstances allowed the use of sensitive data for mitigation of high-risk AI models to prevent bias and discrimination. This exception is now expanded to all AI systems based on the assessment of companies if the processing is necessary (see also above as part of the changes to the GDPR).

This will allow intrusive gathering of your most sensitive personal data to train AI systems. Also see above "Using your personal data for training AI.

While Big Tech claims that more data is necessary for detecting bias, research suggests that debiasing - certain statistical techniques to 'correct' bias in databases that are used to train AI - is often ineffective and is unable to detect the many forms and contexts in which discrimination and bias manifests. Instead, it is a technical fix that enables Big Tech companies to collect yet more sensitive personal data to train their AI models while creating the illusion of ethical AI, all while encouraging the widespread adoption of AI across all sectors of society.

The digital omnibus introduces article 4(a) to the AI Act: "To the extent necessary to ensure bias detection and correction in relation to high-risk AI systems in accordance with Article 10 (2), points (f) and (g), of this Regulation, providers of such systems may exceptionally process special categories of personal data."

Big Tech's lobby position

The tech lobby constantly portrays data protection as a major obstacle to AI training and has therefore repeatedly lobbied, either specifically or in general terms, for the weakening of data protection.

Google: “We propose extending the allowance in Article 10(5) to permit the necessary data processing for bias detection and correction across all AI systems and general purpose AI models. Extending this provision will provide a harmonized legal basis for developers to proactively build the fair, representative, and trustworthy AI that aligns with the EU’s core values and benefits all citizens. It will also reduce the risk of AI models and systems perpetuating or amplifying societal discrimination, irrespective of their specific AI Act risk classification.”

Big Tech lobby organisation **Information Technology Industry Council (ITI)**: “The AI Act's Article 10(5) allowance for special categories of personal data processing for bias mitigation should be extended to the training of all AI systems and GPAI models, not just those classified as "high-risk.”

A Big Tech-far right alliance in the making?

The Commission’s digital omnibus received widespread criticism. Civil society organisations, think tanks, experts, and political groups in the European Parliament from the left to the centre all perceived the Commission’s proposals as handouts to Big Tech and the Trump administration.

But while the Social Democrats in the Parliament called the digital omnibus unacceptable deregulation, far right parties quickly came to the support of the Commission.

Big Tech lobbying of the European Parliament also shifted in higher gear. Lobbying of the far-right seems to have become a particular priority for Meta, and to a lesser extent Google. While during the previous parliamentary mandate, Meta only met once with a far-right MEP, during this parliamentary mandate it has already met 38 times with MEPs from the ECR, the Patriots and the Europe of Sovereign Nations Group. The digital omnibus is a key priority in those meetings. In the week of 8 December 2025, Meta met with four far right MEPs with most of those meetings mentioning the digital omnibus.

Google has also not shied away from meeting far-right MEPs. A few days after the launch of the digital omnibus, Google joined a dinner party in Strasbourg hosted by six French MEPs from the far right Rassemblement National.

Big Tech's lobbying strategy in the US, where it has aligned itself with the Trump administration, now appears to have been extended to the European Parliament.

As outlined in this article, the digital omnibus is not just an unprecedented attack on our digital rights – it also closely mirrors Big Tech lobbying positions. The Commission’s deregulation agenda threatens to undermine years of progress in reining these tech giants and protecting our privacy.

The emerging far right - Big Tech alliance in the European Parliament points towards an even more alarming trend. It should now be clear to all that the Commission’s deregulation agenda isn't just opening the door to Big Tech, it's inviting the far right in.
However, this outcome is not inevitable. The European Parliament now has a crucial opportunity to stop this dangerous proposal and defend the hard-won data protection safeguards.

The Digital Omnibus has received massive pushback, from civil society organsations, from within parliament and from member states, including Malta, which recently requested more time to scrutinise the proposal.

What happens next depends on whether we manage to increase the pressure.

Now is the time to make our voices heard and make it crystal clear to the European Parliament and national governments that they must stand up for our privacy, freedom of expression and democratic control over technology, and reject the Digital Omnibus.