WORKING PAPER | ISSUE 02/2026 | 18 FEBRUARY 2026

EUROPEANS SHOULD BE ALLOWED TO TRADE PERSONAL DATA

PAUL HEIDHUES, NICK JACOBSON, GIORGIO MONTI AND FIONA SCOTT MORTON

The European debate over personal data trading has become trapped between two unworkable extremes: the status quo of allowing platforms unfettered access to user data, or making data sharing so difficult it is effectively banned. Neither position serves consumers' interests. Personal data sharing can create substantial value – enabling relevant advertising and powering digital services – but currently this value is captured almost entirely by gatekeepers, while users surrender control of their commercial, location, social network and even sensitive medical data without meaningful consent or compensation. The critical policy challenge is to enable beneficial data sharing while protecting users' fundamental privacy rights and ensuring they are fairly compensated for data they choose to share.

The solution lies in creating well-regulated data markets. European Union regulators should establish a system that prohibits trading of personal data that is sensitive, sets a default that is both safe and gives users bargaining leverage, and mandates transparent and effective choice architectures to ensure users are informed. When a default allows users to access a platform's free service in a more private way, the platform will have a financial incentive to encourage more data sharing. Platforms will need to compensate users to make active and informed choices to share more data. Platforms may also offer paid options to users who want to opt out of data sharing and to see no ads. This menu of three options – free, subsidised and costly – will allow users to make individual choices about sharing personal data in a safe and regulated environment.

Such regulation would allow platforms to continue advertising-supported business models, while giving consumers genuine control and economic benefit from their data. Without functioning data markets, Europe faces two poor outcomes: either personalised advertising collapses and valuable digital content disappears, or courts permit platforms to continue exploiting users without consent, delegitimising privacy law. Well-designed data markets would enable fairness and contestability by allowing smaller digital competitors to obtain data on the same terms as big ones, and by sharing with users some of the hundreds of billions earned annually by platforms such as Google.

Paul Heidues is ESMT distinguished affiliate professor and a professor at Düsseldorf Institute for Competition Economics
Nick Jacobson is Associate Program Manager of the Digital Economy Project at Yale University's Tobin Center for Economic Policy
Giorgio Monti is a professor at the Robert Schuman Centre for Advanced Studies
Fiona Scott Morton (fiona.scottmorton@bruegel.org) is a Senior Fellow at Bruegel

Recommended citation:
Heidhues, P., N. Jacobson, G. Monti and F. Scott Morton (2026) 'Europeans should be allowed to trade personal data', *Working Paper* 02/2026, Bruegel, available at https://doi.org/10.64153/QHXP9557

1 The issue

The trading[1] of personal data is a controversial policy in Europe, most recently in relation to sparring between internet platforms and data protection authorities over pay-or-consent models[2], in which consumers who don't want their personal data processed would pay fees for advertising and behavioural-tracking-free access to online services. The debate is defined by two extremes: allowing companies unfettered access to user data, or banning data sharing altogether. Neither is reasonable and society will be harmed if a court is required to choose between one side or the other. Policymakers and courts must offer a middle ground.

It is critical to appreciate that the sharing of personal data can bring many benefits to European consumers. For instance, if a consumer in the last few days has searched for flights to Lisbon on a travel website, she may want to be made aware of special offers by a Portuguese hotel. The hotel can reach her through advertising only if the relevant laws and technologies allow the travel website or a third-party tracking system to communicate her interest[3]. Similarly, if she has shown interest in movies, she might want to be made aware of specialised review sites. While there may be problems with the current internet advertising model, this should not obscure the fact that there are also strong benefits to the sharing of data (Bergemann *et al*, 2023). But any social benefit from this system, and significant profit, is captured in large part by the advertising revenues of multi-site platforms such as Google Search, which routinely generates more than $200 billion in annual ad revenue[4]. The profitability of targeted advertising is well understood.

In the current regime, the data exploited by gatekeeper platforms is comprised of users' commercial personal data (eg shopping), their location data, their social networks, the type of personal data that the European Union General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) distinguishes as sensitive (eg medical treatments) and more[5]. Wernerfelt *et al* (2024) showed that advertising on Meta that is targeted using personal data from outside Meta (such as a web search for 'flights to Lisbon') sells at a higher price than ads which do not use that data.

The regulatory issue is whether such tracking and sharing violates a user's fundamental right to privacy, as well as other laws. Such a right to privacy, in theory, means that users' personal data is not tracked and shared unless they provide informed consent. The 'default', as it were, is not to share

---

[1] The term 'trading' does not properly apply to data. In a normal trade, the seller of a good has no access to it after the trade. By contrast, data is usually still available to the party that sells it. Furthermore, we include under trading the fact that an individual accepts that a platform uses the data it acquires for particular purposes – which is not, properly speaking, trade. However, this terminology has become commonly used.

[2] Anupriya Datta, 'Meta to tweak its pay-or-consent ad model for EU users in January', *Euractiv*, 8 December 2025, https://www.euractiv.com/news/meta-to-tweak-its-pay-or-consent-ad-model-for-eu-users-in-january/.

[3] There are numerous technologies that can track users such as cookies, pixels, mobile IDs and signifiers, and more advanced browser or device fingerprinting. See Jacob Roach, 'Here's What Your Browser Is Telling Everyone About You', *Wired*, 16 October 2025, https://www.wired.com/story/what-is-browser-fingerprinting/.

[4] Jeremy Bowman, 'How Much Does Google Make in Ad Revenue?' *The Motley Fool*, 24 October 2024, https://www.fool.com/investing/2024/10/24/how-much-does-google-make-in-ad-revenue/.

[5] See GDPR Article 9, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e2051-1-1.

personal data without a proactive choice by the user. Critically, if regulation removes the ability of a digital business to monetise through targeted advertising by restricting automatic tracking, some businesses might find that some services become less profitable and thus reduce the provision of content that is valuable to consumers. On the other hand, if users have the right to control their personal data and many of them choose not to share it, stealing that data through tracking imposes a loss on consumers. Below we explain how to balance these concerns.

There may be businesses at the margin that, facing any diminution in the amount of freely harvested personal data, will lower the quality of their content. Many of the platforms that harvest the most personal data, however, are 'gatekeeper' platforms, defined under the EU Digital Markets Act (DMA, Regulation (EU) 2022/1925) to be both large and economically important. Indeed, several of these platforms are alleged, or have been found, to have violated the antitrust laws in either Europe or the United States (Google Search, Google ads, Meta, Amazon, Apple)[6]. These platforms earn tremendous economic profits and are unlikely to be near this margin (Competition and Markets Authority, 2020). More fundamentally, if users' personal data is theirs to control, data collectors such as platforms must seek permission to collect and use that data through a voluntary arrangement that suits and benefits both parties. Consumers should gain if they choose to share their data, monetarily or otherwise.

Since digital platform services are typically offered at a price of zero, how can users be compensated for their time and data[7]? The answer is that the competitive price for digital platforms may well be negative once the value of personal data is factored in. Designing and operating a functional data market would raise a number of challenges, including how to organise consumers (perhaps through data intermediaries) to enable efficient transactions at scale and what obligations such intermediaries would have to users[8]. While we discuss some of these challenges below, our proposal is most immediately practical for those companies that already collect and monetise user data at sufficient scale such that some compensatory exchange could be possible. Putting a price on data would entail a platform making an offer of compensation when it requests user consent for personal data. Users could then freely choose to accept or reject this offer without implications for the services the platform may provide.

Note that, so far, our discussion and examples focus on the trading of data for targeted advertising purposes. There are other reasons why data might be traded or exchanged (see the discussion of data spaces in section 5). Advertising, however, is probably the most controversial use because it is so

[6] For some examples, see: United States of America vs Google LLC, Case No. 20-cv-3010 (APM), https://files.lbr.cloud/public/2024-08/045110819896.pdf, United States vs Google LLC, Case 1:23-cv-00108-LMB-JFA, https://oag.ca.gov/system/files/attachments/press-docs/Google%20AdTech%20decision.pdf, Epic Games Inc vs Apple Inc, Case No. 4:20-cv-05640-YGR, https://www.documentcloud.org/documents/21060696-epic-v-apple-ruling/, and European Commission press release of 14 November 2024, 'Commission fines Meta €797.72 million over abusive practices benefitting Facebook Marketplace', https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_5801/IP_24_5801_EN.pdf.

[7] Such a system might be similar to the way credit-card companies reward their users.

[8] We have further delineated some conditions for market design in Bergemann *et al* (2023).

pervasive and because it has widespread potential to expose users to third parties through targeting[9]. For this reason, we continue to focus on advertising.

2 Two extremes

While a compensation scheme would itself be subject to discussion, the policy debate is nowhere close to considering an outcome that involves trading. Instead, the debate is dominated by two opposing visions. On one side are privacy advocates who fear that letting people 'sell' their personal data will lead to exploitation and a violation of their fundamental rights; on the other side are digital platforms that want the unfettered ability to collect personal data to feed services, including advertising, that utilise it.

Some on the privacy side advocate positions that would make the processing of personal data so cumbersome that it would threaten the provision of digital content or the availability of digital services. For example, European Digital Rights (EDRi) has suggested replacing targeted advertising online with contextual or low-context ads (Lemoine *et al*, 2021). While the scale and scope of data collection for numerous and opaque purposes is problematic, ending personalised online advertisements would eliminate a large share of the market surplus. It also leaves no pathway for consumers to share the surplus currently captured almost entirely by platforms.

European Data Protection Board (EDPB)[10] guidelines published in 2019 on Article 6(1)(b) General Data Protection Regulation (GDPR), paragraph 54, said:

> *"Considering that data protection is a fundamental right guaranteed by Article 8 of the Charter of Fundamental Rights, and taking into account that one of the main purposes of the GDPR is to provide data subjects with control over information relating to them, personal data cannot be considered as a tradeable commodity"* (EDPB, 2019).

The EDPB explained that under the GDPR, a high level of user consent is required for personal data to be processed. This 'hassle cost' will make users unlikely to go through the agreement process without a good reason. The EDPB also seems to want platforms to offer their existing service in a version that does not process any personal data and has a zero price[11]. If a platform must ask for the user's consent, but only offer the same version of the service with no additional benefit, then there would be no reason for a user to consent to share data in that situation. The inability to offer any benefit in

[9] See, for example, Tanya O'Carroll's lawsuit in the United Kingdom against Facebook, in which a hired expert managed to identify and target her specifically with an advertisement using Facebook's ad system, a feat she said Meta told her was impossible. See Grace Dean, 'Facebook to stop targeting ads at UK woman after legal fight', *BBC News*, 22 March 2025, https://www.bbc.com/news/articles/c1en1yjv4dpo.

[10] The EDPB is a committee comprised of each European Union member state's data protection authority.

[11] A 2024 EDPB opinion conveyed mixed messages on this issue. On one hand, it appeared to allow developers to charge a reasonable fee for an alternative that does not include behavioural advertising. On the other, it maintained that "*If controllers choose to charge a fee for access to the 'equivalent alternative', controllers should consider also offering a further alternative, free of charge, without behavioural advertising, e.g. with a form of advertising involving the processing of less (or no) personal data*" (EDPB, 2024).

exchange for more data sharing threatens business models that rely on non-exploitative, behavioural advertising for revenue.

At the other extreme, the largest ad-supported digital platforms have for years used a business model in which they process personal data without clear explanations (in some cases, allegedly deceiving users), without offering a realistic choice should the consumer not want to share their data, and without direct compensation for its monetisation. Platforms argue that personalised advertising has benefits for consumers[12]. This can certainly be true to some extent, but this basic principle does not imply that the current sharing of surplus between platforms, consumers and advertisers is in any sense optimal from a societal viewpoint.

In 2025, the European Commission rejected (under the DMA) Meta's 'compliance' model of offering users a high-priced alternative as the only option to avoid full data collection and use practices on Facebook and Instagram – what observers dubbed 'pay or consent', or 'pay or OK'[13]. The decision reiterated that EU law requires consumers to be given more control over the use of personal data than dominant platforms have so far offered.

3 Labour as an analogy

A middle ground is both sensible and easy to envision. Defining a middle ground in data trading when such healthy markets hardly exist today can be clarified by analogy with a more developed market: labour. The EU right to freedom of movement seems to us at least as important as the right to privacy.

Consider the following analogy: Europeans have a fundamental right to control the movement of their bodies[14]. This fundamental right creates a problem for an employer, who would like to hire a worker to, for example, drive a digger as part of a road repair crew. The employment contract requires the worker to sit in the digger all day from 0800 to 1200 and from 1300 to 1700. The worker is not physically restrained, of course, and is able to exercise their right to move by climbing down from the digger and leaving it before the workday is over. If they choose to do that, however, the employer will punish the worker by withholding income or even firing them. The risk of losing something as significant as a job

[12] In its statement announcing changes in response to European regulation, Meta argued that "*Offering a choice between a paid subscription and free access to a service funded by personalised ads is a well-established business model and a valid legal consent choice under EU law . . . Each €1 spent on Meta ads yields €3.79 in advertiser revenues in Europe. This value is only available through personalised advertising but is at risk of decline because if EU regulation makes digital advertising less efficient, the entire European business community suffers*". See Meta article of 12 November 2024, 'Facebook and Instagram to Offer Subscription for No Ads in Europe', https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/. Google's 'Personalized advertising' policy begins, "*Personalized advertising is a powerful tool that improves advertising relevance for users and increases ROI for advertisers. Because it works by employing online user data to target users with more relevant advertising content, it can provide an improved experience for users and advertisers alike*". It goes on to acknowledge that "*certain interests are sensitive and that targeting based on them could negatively impact user experience*" but does not indicate any interest in trading data. See Google website on personalised advertising, https://support.google.com/adspolicy/answer/143465?hl=en.

[13] See European Commission press release of 23 April 2025, 'Commission finds Apple and Meta in breach of the Digital Markets Act', https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085.

[14] See Articles 1, 3, 5, and 6 of the Charter of Fundamental Rights of the European Union, https://eur-lex.europa.eu/eli/treaty/char_2012/oj/eng.

constitutes financial coercion. The worker's salary therefore operates as financial coercion to give up free movement and stay on the job. This means that the worker does not truly have the freedom to move and leave the road repair crew mid-shift. Hence, the worker's fundamental rights are violated by being employed.

Strictly following this reasoning leads to the conclusion that employment is illegal. Many people, however, are legally employed by corporations throughout Europe – and both workers and corporations gain from that arrangement, which entails compromising some freedom of movement for income. Just as a ban on the restriction of freedom of movement described above would shut down labour markets that bring tremendous benefits to citizens, broad bans in data trading would shut down digital markets that could likewise bring users value.

On the other hand, the labour market analogy also demonstrates the problem with the invasive actions taken by some digital platforms today. In modern labour markets, firms are not allowed to contract with workers to do anything under any conditions for any amount of compensation. The critical element is the possibility to *regulate* sensitive markets. Without any regulation, labour agreements can result in exploited workers. Similarly, major platforms' current data policies, many of which have yet to comply with the law, may be exploiting users.

It matters a great deal whether the market is effectively regulated in a way that ensures consumers are not exploited. Modern societies have adopted strong protections for workers in their labour laws, and this is one reason why trade in labour is so common. Child labour is difficult to make beneficial for the worker, so governments have shut down most of that market over the last one hundred years. Modern labour regulations also prohibit indentured servitude. Meanwhile, they mandate overtime pay, vacations and workplace safety standards, establish protections for unions, make discrimination and harassment illegal, and more. Such regulations go a long way towards ensuring that the labour market benefits the individuals who participate in it – thus supporting and encouraging people joining the labour force[15]. As technology and society change, those regulations continue to evolve to protect workers from exploitation. For example, recent European regulations govern an employee's email responsibilities outside of working hours or how an employer must choose shift schedules[16].

Recognising and securing a fundamental right is, therefore, not the same as banning all trading thereof. When trading something covered by a fundamental right can be made safe, the freedoms secured under such a right can become, to a limited extent, alienable, as a person's freedom of movement can be affected by their choice to accept paid employment. More generally, it is appropriate to allow for trade within areas covered by fundamental rights when substantial welfare can be gained without

[15] The appropriate breadth of regulation in labour markets remains subject to debate, but it is uncontroversial that the protections we list here should be provided to some degree.
[16] Dominic Hauschild and Brian Carey, 'Could work emails be banned after 5pm – and how do other countries do it?' *The Times*, 1 June 2024, https://www.thetimes.com/business-money/companies/article/right-to-disconnect-rules-company-emails-wfh-0qb6qsk6r. The German Federal Institute for Occupational Safety and Health (BAUA) provides guidelines for night and shift work to employers based on the German Working Hours Act, 'Organisation of Night and Shift Work', undated, https://www.baua.de/EN/Topics/Work-design/Working-time/Night-and-shift-work.

endangering the citizen, perhaps because of appropriate regulations. In this context, we argue that data trading should be permitted when it is carried out by fully informed consumers making a careful and free choice in a regulated environment, and where the default choice gives the consumer enough bargaining power to obtain an appropriate share of the surplus.

A major barrier to this solution is that digital platforms have been earning huge profits by targeting advertising based on personal data and therefore have no interest in a regulated market for personal data. Platforms do not want to explain carefully to consumers what data they collect or to give consumers a choice about whether to share it or not, and they particularly do not want to have to compensate individuals for sharing data the way an employer has to compensate workers for their labour. By revealed preference, the *status quo* is more profitable for platforms. Rather than offering compensation that satisfies both sides, they defend the status quo by arguing that protective interpretations of current law would result in shutting down the use of personal data and are thus unreasonable or disproportionate in their impact.

A second barrier to adopting a market-based solution is consumer adoption and understanding. Consumers will have no idea, *ex ante*, how much harm they can prevent by denying data use (eg by exploitative financial products) nor how much they can be paid by sharing some personal data (eg for a search for a pair of shoes). Consumers may care whether a nonprofit they like or a company making huge profits for shareholders uses their data. But each user will need time in a new market to learn what level of data sharing at what price is most attractive to them. This is a common process for consumers who enter a new market, such as with the purchase of a car.

4 The challenge for regulators

Regulators are failing consumers by not putting forward a safe way to make data markets work. Such regulation would identify personal data too dangerous to trade and forbid those transactions. The regulator would have the power to oversee the choice architecture that platforms must use for consumers to make free and informed choices. Likewise, the regulator could mandate that certain levels of privacy be offered in various versions of the service. Such a framework would allow courts to find that default privacy settings were proportionate because they allow an advertising-supported business model to continue while, at the same time, protecting consumers in terms of both the economic value and data they give up. Regulated trade would allay the concern that privacy rules harm businesses unreasonably or are not proportional. Platforms could buy the data they value from consumers who are willing to share it. If consumers were not willing to let their data be used at a price that the platform was willing to pay, then it would be efficient to have no trade in that instance. At the same time, regulation of these transactions would protect consumers and their fundamental rights.

We know from the statements, behaviour and market valuations of major platforms that personal data is tremendously valuable[17] – and yet policymakers are not setting rules that allow consumers to share in that value. Today, users effectively have no choice but to agree to gatekeepers' terms and conditions that lump all data together and allow the user to be tracked around the internet as a condition of using a 'free' service. Without 'agreeing' to the platform's data policy, the user cannot access its services – services for which there are no good substitutes because of the market power of the platform. This coercive system does not give users effective choice, nor does it offer them economic reward. The rules in the DMA are designed in part to remedy the lack of contestability and fairness in the market for personal data.

As mentioned above, at present no one knows what amount of personal data will trade at what prices because the market is completely new. The preferences of citizens for privacy – once they face real choices involving money and credible enforcement – are unknown, and there are few convincing benchmarks. Here, the well-known 'privacy paradox' creates confusion and concern for regulators. The 'privacy paradox' is the contrast between users saying they care a great deal about keeping personal information private and evidence that consumers will agree to pay very low sums to obtain privacy[18]. Regulators then wonder which of the two expressed preferences is relevant? Part of the problem is the huge variation in choice environments across these different experiments and the lack of transparent real-world consequences for user choices[19].

Because of the risk that choice architecture can be designed so that the platform steers consumers to the choice the platform wants (eg by using dark patterns), the environment must be regulated. For example, is one of the choices presented first, in larger type, pre-selected or otherwise favoured? If so, users will disproportionately choose it. But substantial progress can be made on this issue with platform A/B testing and experimentation. By reviewing how different designs of the choice architecture affect consumer choice, through following consumers *ex post*, interviewing them and developing metrics for welfare, a regulator can require platforms to use choice architecture that is more neutral. By requiring platforms to offer neutral, clear and relatively simple choices, consumers have a better chance of choosing a data environment that reflects their true underlying preferences. These are the kinds of rules regulators need to develop so that consumers who exert reasonable effort can make informed data-sharing decisions.

---

[17] The 2024 net incomes of Google and Meta combined were €149 billion. Likely around 20-30 percent or €30 billion to €45 billion is earned in Europe.

[18] See Acquisti *et al* (2020) for a review of the vast literature on the privacy paradox in the social sciences. The authors argue that much of the literature *"confuse*[s] *wants with opportunities,"* and that the ability to achieve desired privacy protection online is excessively difficult for both economic and psychological reasons.

[19] Consumers, in the current choice environment, are typically unable to grasp fully what profiling is possible based on specific cookies and do not take the time to read the description of various cookies for every website they visit. Furthermore, users may presume that their personal information is already 'out there' somewhere and, while they would be willing to pay for privacy, presume this is moot when considering a single digital service. As a result, they may incorrectly look as if they have no preference for privacy. In addition, many digital services periodically change their terms of usage. If consumers incur switching costs when changing their service provider, current privacy levels may be undone in the future when users are locked in, making users reluctant to pay for them.

The biggest platforms have so many interactions with users and collect so much personal data that they can carry out data transactions bilaterally (that is, without the need for a data intermediary to achieve scale). For example, Google could offer a menu of options varied by personal data collection and benefits. A small website that a consumer visits only once will, on its own, not be able to make such a market work. A well-designed, regulated framework in the EU could overcome these issues and a market would surface prices at which users offer their data whenever they value their privacy less than the benefits offered by the platform. Artificial intelligence agents hold promise in this regard and might be able to remove frictions by carrying out a consumer's instructions each time a decision had to be made, but we recognise that building such a framework is far from easy.

Markets have the great advantage over regulation in accommodating variations in how much consumers value keeping their data private. For example, at a given price, a member of a security force may not want to share location data while a college student is happy to; a newly pregnant woman, in contrast to other women offered the same benefit, may not want to share shopping data. In a market, consumers placing a high value on personal data may choose not to trade it.

Platforms would set the prices or benefits they offer to attract customers, recognising this variation (the supply curve). Critically, as in labour or consumer markets, society may want to protect participants from certain exploitative practises. Regulators will likely want to preclude children from being targeted based on personal information, limit the ability to target predictably addicted citizens with ads fostering their addiction or prevent sharing of sensitive data. Therefore, some data trading will be banned for user safety[20]. Because the understanding of which data is sensitive can evolve over time, it could also be reasonable to time limit the storage of personal data. Data for targeted ads loses value rapidly as time passes – which is why platforms continuously collect more – so such a rule is not very costly to advertisers.

Both the GDPR and the EU Digital Services Act (Regulation (EU) 2022/2065) already ban or more severely restrict trade in sensitive data concerning religion, health, sexuality and the like. Such reasonable provisions protect[21] users from harm they may not be able to foresee. We stress that such bans are very common in other areas of modern economies. For example, trade in dangerous foods, medicines and automobiles is often banned. Another set of limits could concern the use of collected personal data to reduce the risk of leakage into dangerous applications of data by foreign governments, bad actors, or other unauthorised parties (which could have consequences for, say, AI training with personal data).

[20] We also note the various uses of data collected for one reason or is then used for purposes to which users likely would never have consented. One example might be Palantir's construction of an AI tool that ostensibly identifies potential targets for US Immigrations and Customs Enforcement. See Caroline Haskins 'ICE is Paying Palantir $30 Million to Build "ImmigrationOS" Surveillance Platform', *Wired*, 10 April 2025, https://www.wired.com/story/ice-palantir-immigrationos/.
[21] Note that these restrictions come at a cost. Some users might appreciate advertising that provides information that enriches their religious practices or that helps them manage health issues.

5 Possible data market design

One proposal is that a gatekeeper that wants to collect personal data and use it for advertising should offer consumers a menu with minimal data processing as a zero-fee option, more-intensive tracking and processing as a subsidised option and no data processing as a paid option (Monti, 2025). Consumers would then have the option of using the (same) service by either (a) paying no money and accepting a low level of processing and targeting with regard to most data, (b) accepting a benefit in exchange for being tracked around the internet, or (c) paying a price to have no data collection and see no ads. In (b), the consumer would be paid to share a specific, regulated, transparent amount of personal data.

Europe has some laws designed to foster the creation of data markets. In 2020, the Commission's European strategy for data explicitly set out the vision of a 'Single Market for Data' in which information can move freely across sectors and borders, while fully respecting the GDPR (European Commission, 2020). The Commission argued that overcoming the widespread reluctance to share data requires a framework of clear, trustworthy and privacy-preserving governance and regulation.

One piece of this vision is common European data spaces: sector-specific ecosystems (in areas such as health, mobility and energy) designed to connect data providers and data users while ensuring that participants retain control over their data[22]. Within these spaces, both personal and non-personal data can be shared under secure and privacy-preserving conditions. Crucially, data spaces also allow for commercial data sharing, creating the institutional foundations for what was intended to evolve into a genuine single market for data (Bisière *et al*, 2025). EU funding supported the initial development of data spaces, but this support was never meant to be permanent. Now, participating companies struggle to identify sustainable business models. Few data spaces are fully operational or mature as of today. The difficulty of devising rules and governance structures that make participation attractive makes truly universal data spaces aspirational at present.

The Data Governance Act (DGA, Regulation (EU) 2022/868), in force since 2023, could be assumed to aid in creating healthy data markets because it defines a legal framework for data intermediaries. By providing technical and legal infrastructure for data exchange, intermediaries are intended to serve as matchmakers or brokers between the data demand and supply side. Under this regulation, however, data intermediaries are prohibited from profiting themselves from trade in data. The lack of a business model limits possible entrants. GDPR also prevents users from delegating their privacy choices to a

[22] See European Commission, 'Common European data spaces', undated, https://digital-strategy.ec.europa.eu/en/policies/data-spaces.

third party, which can be interpreted to mean that a data intermediary has limited usefulness[23]. In addition, there is legal ambiguity surrounding what exactly constitutes a data intermediary.

More generally, regulatory fragmentation and vagueness have hampered the emergence of European data markets. Different pieces of legislation introduce distinct concepts and obligations, sometimes without full alignment. Combined with the overarching precedence of the GDPR, this patchwork has created legal uncertainty rather than solutions. The lack of a regulatory framework means that a smaller business that hypothetically wants to offer a benefit to users in exchange for personal data has no market infrastructure to use, while the value of the trades it wants to make are too small to justify building one. Google and Meta, by contrast, traffic in so much personal data that such infrastructure is worth building. Indeed, both gatekeepers have already created settings that consumers can use to limit some aspects of personal data processing.

The Digital Omnibus initiative – a simplification and streamlining proposal – that the European Commission published in November 2025 is one attempt at responding to the regulatory complexity[24]. If enacted, it would pare back some hurdles by eliminating some of the restrictions on data intermediaries described above and transforming what was a mandatory registration system for such intermediaries into a voluntary one, thus allowing for more profitable business models. The DGA itself would be formally eliminated and its surviving provisions incorporated into the Data Act (Regulation (EU) 2023/2854). However, the Omnibus proposal falls short of offering a comprehensive solution for healthy data markets.

The missing attribute in current discussions is the element of trading between the platform and the subset of users who are happy to share data. EU regulators should come around to using the reform of current regulations to enable safe data trading so that consumers gain in privacy and in benefits, while platforms are free to carry out an ad-supported business without violating fundamental rights.

6 Conclusion

If citizens cannot access a well-functioning data market, then they cannot benefit from control over their personal data. The current two options – neither of which is compatible with a market – could lead digital services in Europe towards one of two extremes: either personalised advertising markets will shut down and consumer content will decrease, or courts and regulators will find ways to allow the platforms to continue to process personal data without permission. This second option – which we think is more likely – will de-legitimise the law, while allowing the current exploitation of consumers to continue.

[23] Although, it may be acceptable for users to instruct an agent to carry out their preferences using automated consent tools. For an example of innovation in this area see the ErnieApp website, https://ernieapp.com/.
[24] See European Commission press release of 19 November 2025, 'Simpler EU digital rules and new digital wallets to save billions for businesses and boost innovation', https://digital-strategy.ec.europa.eu/en/news/simpler-eu-digital-rules-and-new-digital-wallets-save-billions-businesses-and-boost-innovation.

Both of these would be negative outcomes for consumers. Thus, it is critical to outline to courts and regulators a different option that adheres to the law and supports content on the internet. This option is all the more important since the largest incumbent firms already have access to large troves of data. Their competitors need to acquire data to have a chance to challenge them. Such challenges can only happen with a well-regulated market for data. Regulations that allow users to refuse to share personal data give users a way to force platforms to offer them a better bargain.

References

Acquisti, A., L. Brandimarte and G. Loewenstein (2020) 'Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age', *Journal of Consumer Psychology* 30(4): 736–758, available at https://psycnet.apa.org/doi/10.1002/jcpy.1191

Bergemann, D., J. Crémer, D. Dinielli, C.-C. Groh, P. Heidhues, M. Schäfer ... M. Sullivan (2023) 'Market Design for Personal Data', *Yale Journal on Regulation* 40(3), available at https://www.yalejreg.com/print/market-design-for-personal-data/

Bisière, C., J. Crémer, B. Jullien and Y. Lefouili (2025) 'The Economics of Data Spaces', *Policy Paper*, July, Toulouse School of Economics Digital Center, available at tse-fr.eu/sites/default/files/TSE/documents/DigitalCenter/policy_paper/the_economics_of_data_spaces_july_2025_policy-paper.pdf

Competition and Markets Authority (2020) *Online platforms and digital advertising*, available at https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf

EDPB (2019) 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects', European Data Protection Board, available at https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

EDPB (2024) 'Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms', European Data Protection Authority, available at edpb_opinion_202408_consentorpay_en.pdf

European Commission (2020) 'A European strategy for data', COM(2020) 66 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020DC0066

Lemoine, L., E. Jakubowska, A. Belu and D. Naranjo (2021) *Targeted online: An industry broken by design and by default*, European Digital Rights (EDRi), available at https://edri.org/wp-content/uploads/2021/03/Targeted-online-An-industry-broken-by-design-and-by-default.pdf

Monti, G., J. Crémer, A. Fletcher, P. Heidhues, N. Jacobson, G. Kimmelman and M. Schnitzer (2025) 'Compliant Use of Personal Data for Advertising on Social Networks in Europe by Gatekeepers', *Policy Discussion Paper* No. 11, Yale Tobin Center for Economic Policy, available at https://tobin.yale.edu/research/compliant-use-personal-data-advertising-social-networks-europe

Wernerfelt, N., A. Tuchman, B. Shapiro and R. Moakler (2024) 'Estimating the value of offsite tracking data to advertisers: Evidence from Meta', mimeo, available at https://doi.org/10.2139/ssrn.4176208

Bruegel, Rue de la Charité 33, B-1210 Brussels
(+32) 2 227 4210
info@bruegel.org
www.bruegel.org