# SIX YEARS OF THE GDPR: PRICED OUT OF PRIVACY?

accessnow

Access Now defends and extends the digital rights of people and communities at risk. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

**This paper is an Access Now publication.** It was written by Chiara Manfredini, in collaboration with Daniel Leufer. The authors would like to thank the Access Now team members who provided support, including Méabh Maguire, Loren Giordano, Eliška Pírovká, and Caterina Rodelli.

For more information, please visit:
**https://www.accessnow.org**

Contact: **Chiara Manfredini** | EU Policy Associate
**chiara@accessnow.org**

**Published in November 2024**

# INTRODUCTION

The General Data Protection Regulation (GDPR) entered into application six years ago. Since then, multiple enforcement challenges have surfaced, including a rise in companies deploying so-called "pay or consent" business models, which force people to pay to enjoy their own right to privacy and data protection. This worrying trend is the focus of our report.

The fundamental premise of a "pay or consent" model sees a company that provides online services (e.g. a social media platform) presenting the people who use its services with a "choice" over how to access those services.[1] On the one hand, people can pay a fee to use the service *without* their personal data being used for a specific commercial purpose (e.g. being invasively tracked and surveilled for the purposes of targeting ads), as stated by the company. On the other hand, those who cannot, or will not, pay this "premium" fee may still use the service, but in exchange they must agree to their personal data being processed and used for those specific commercial purposes. In essence, those who do not pay in currency must pay with their privacy, if they want to keep using the service in question.

This report specifically looks at the impact of using "pay or consent" models to force people to agree to behavioural advertising, which involves extensive monitoring and exploitation of people's online activities.[2] By observing and tracking what people do online, companies collect enormous amounts of data from different sources across different websites.[3] This data is then used to create detailed "advertising profiles", which are in turn used to target people with ads that match their inferred interests.[4]

"Pay or consent" models, paired with behavioural advertising, harm people and their human rights by:

- **Coercing consent:**[5] The GDPR is intended to give people control over their data. The GDPR establishes six legal bases that a company can use to process personal data, one of which is consent. This allows companies to process personal data from people who have "freely given" their consent, which must be as easy to withdraw as it is to give. The European Data Protection Board (EDPB) has emphasised that when providing consent, people must have a real choice, with no risk of deception, intimidation, detriment, or coercion.[6] This definition is supported and reiterated in other EU laws. "Pay or consent" models are therefore at odds with the GDPR's very basis, since they instead operate on the assumption that the data belongs to the

[1] EDPB Opinion on Pay or Consent, page 9.
[2] EDPB Guidelines 8/2020 on the targeting of social media users, paragraph 3; Article 29 Data Protection Working Party Opinion 2/2010 on online behavioural advertising, page 7.
[3] EDPB Opinion on Pay or Consent "Description of pay or consent models", page 9-10, EDPB Guidelines 8/2020 on the targeting of social media users, paragraphs 3, 10, and 11.
[4] Ibid.
[5] See from Noyb (2023): "More than 99 percent of people decide against a payment when faced with a "privacy fee." *Noyb files GDPR complaint against Meta over "Pay or Okay"*.
[6] EDPB Guidelines on Consent, page 13.

companies, rather than to individuals, and that in refusing consent, people are taking something away from the companies.

- **Forcing behavioural advertising on people:** "Pay or consent" models enable companies to deprive people of their right to choose and, as a consequence, oblige people to endure the harms of behavioural advertising. Some of the EU's highest authorities recognise behavioural advertising as a particularly intrusive practice that jeopardises individuals' fundamental rights and freedoms.[7] This practice replicates and multiplies existing societal harms, including: infringing data protection rules; deepening discrimination and exclusion; interfering with people's freedom of choice and undermining their autonomy; manipulating people's freedom of thought and opinion; and increasing the likelihood of security risks.
- **Turning privacy from a right into a luxury good:** These models turn privacy into a commodity, causing collective societal harm on two fronts. Echoing what Access Now and Noyb, as well as the EDPB and EDPS, have said, Members of the European Parliament (MEPs) have affirmed that "*human rights are universal, inherent and inalienable aspects of human dignity and personhood (...) and ought not to be subject to commercial transactions*." These models therefore contradict the very essence of the right to privacy and data protection of people, putting them directly at odds with the Charter of the EU.[8] Moreover, by making privacy a luxury, "pay or consent" models deepen existing online discrimination, widen the digital divide, and further reinforce social inequality. As 39 MEPs have said, when you put a price on privacy, you perpetuate "*an unjust system that disproportionately affects those who may already be marginalised or disadvantaged*." Accepting these models as legal would represent an unprecedented and drastic downgrading of our understanding of privacy as being an inalienable right for all people, worldwide.

This report touches on human rights abuses stemming from data exploitation and behavioural advertising, viewed through **the lens of consent**, its meaning, and its purpose. By focusing on what empowers people to exercise their agency online, or what prevents them from doing so, we examine how these models affect one of the main objectives of the GDPR: giving people control over their data.

"Pay or consent" models present challenges to privacy that drive right to the heart of the surveillance-based business model. Many believed the GDPR would have meant the end of this incredibly intrusive practice, or at least a drastic change to it. However, the way the "pay or consent" issue has been dealt with shows this was not so evident. The debate on "pay or consent" models dates back to the drafting of the GDPR, and since then, companies have exploited a lack of clear-cut answers to key outstanding questions within the GDPR, as well as complicated GDPR enforcement practices, to roll out various "pay or consent" practices. Utrecht University's Christina Santos and others have clearly illustrated how these models spread across all sectors. Meta's recent implementation of such a

[7] Court of Justice of the European Union (CJEU) Meta vs. Bundeskartellamt judgement, paragraph 118; EDPB Urgent Binding Decision on Meta, page 46, paragraphs 175 and 197.
[8] Article 7 and 8 of the *European Charter of Fundamental Rights*; reiterated in Article 12 of *Universal Declaration of Human Rights (UDHR)* and Article 8 of the *European Convention of Human Rights*.

model, which other platforms have replicated, shows the urgent need for a clear prohibition to this abuse of privacy.

While the EDPB, following a call for clarity made by national data protection authorities (DPAs), has partially addressed this issue as relates to large online platforms, we are still lacking comprehensive guidelines. Meanwhile the European Commission's investigation, brought under the Digital Markets Act (DMA), the complaints brought by Noyb under the GDPR, and the complaint brought by the European Consumer Organisation (BEUC) under consumer law and data protection, are ongoing. We urgently need a definitive answer on this matter, to prevent further exploitation of people's rights.

The GDPR is at a turning point. We must decide whether to let it reach its full potential or to discard more than a decade of work. The question remains: which direction will the EU take?

As a new European Commission prepares to take office, it is essential to keep human rights at the centre of the EU's work. The outcome of the "pay or consent" discussion is pivotal for strengthening the EU's obligation to protect fundamental rights and freedoms, and showcasing its ability to use existing data protection tools and mechanisms to meaningfully safeguard digital rights.

**We urge the EU to address the root causes, and not merely the symptoms and side-effects, of "pay or consent" models**.

This report first sets the discussion of "pay or consent" models in context, analysing how they emerged, and how laws and authorities have responded to them so far. In order to help policy makers, regulators, and legislators make informed decisions that respect human rights, the Charter of the EU, and the GDPR, we then provide the European Commission, the EDPB, and EU enforcement authorities with our recommendations on the topic.

*Please note: this report reflects policy developments and discussions related to "pay or consent" models that emerged before September 2024. Any subsequent developments are not included in the scope of our analysis.*

# II. "PAY OR CONSENT" MODELS: THE SAGA SO FAR

At first glance, "pay or consent" models appear to have emerged relatively recently and suddenly within the EU-wide discourse on privacy, triggered by Meta's EU rollout of such a model in October 2023. However, this model is far from new; many platforms have been using similar models for years. Recitals 42 and 43 of the GDPR, as well as Article 7(4), arguably protect people from "pay or consent" situations, but since they do not explicitly state that consent is invalid if payment is required to refuse it, this leaves a small window for interpretation.[9]

[9] See, European Commission Proposal for the GDPR (25 January 2012) Article 7, paragraph 4.

Meta's "pay or consent" story also predates October 2023. On the first day that the GDPR came into application in 2018, Noyb filed a complaint, questioning whether Meta could use legitimate interests for processing personal data for behavioural advertising. After five years of back-and-forth between national DPAs, it was clarified that Meta *cannot* rely on legitimate interests as a basis for such data processing, as it is deemed too intrusive.[10] Meanwhile, in 2019, Germany's Competition Authority ruled that Meta's (formerly Facebook Inc.) terms and conditions exploited its dominant market position, violating the GDPR by processing data without a valid legal basis. Upon appeal, the case was referred to the Court of Justice of the EU (CJEU), which confirmed that competition authorities can rule on the compliance, or non-compliance, of the undertaking with the GDPR in the context of a decision on abuse of dominant position. The Court also provided further criteria for interpretation including how this aspect can influence "freely given consent".

In November 2023, the EDPB banned Meta from using contract and legitimate interests as a legal basis for behavioural advertising, directing Meta to the need for "freely given consent". Meta responded with a new policy; introducing "pay or consent" models that force users to pay for their privacy, essentially allowing the company to continue processing data without a valid legal basis. Several different complaints, related to GDPR incompatibility and breaches of consumer law, soon followed. In 2024, the European Commission launched an investigation under the DMA and warned Meta about a possible breach of consumer law. All of these initiatives place "pay or consent" models at the centre of the privacy discourse.

In many ways, the current Meta saga has merely brought to light multiple long-standing issues that have gone unaddressed for too long, the most significant of which has been a **lack of a firm, decisive, and harmonised EU-wide response to abusive "pay or consent" models.**

In the years since the GDPR has entered into application, case law and legislative processes have raised questions about where the law stands on "pay or consent" models. The EU's response has been overly siloed, creating even more confusion.

For example, the DMA, in its limited scope, supports the GDPR's meaning of consent and places even stronger obligations on gatekeepers, going as far as to stipulate that they cannot make the use of a service or certain functionalities conditional on user consent, as confirmed by the Commission's preliminary findings. The Commission's Cookie Pledge initiative, although not legally binding and since dropped, also showed the Commission's support for the GDPR and the EDPB's meaning of consent. This initiative would have seen businesses pledge support on a voluntary basis for principles related to cookies and targeted advertising. However, there are also examples of processes that went the opposite direction. For example, the wording of the Directive on Contracts for the Supply of Digital Content and Digital Services, which was discussed just before the GDPR entered into force, seemed to suggest that "pay or consent" models might be legal. But the EDPS Opinion on the same law clearly

[10] Court of Justice of the European Union (CJEU) Bundeskartellamt case, paragraph 118; EDPB Urgent Binding Decision on Meta, page 46, paragraph 175 and 197.

stressed that the GDPR will, in any case, take precedence over the Directive, warning against equating personal data with money and emphasising that data should not be commoditised. Such examples show how addressing issues in a siloed way can create confusion and weaken existing human rights protections.

This state of affairs has been worsened by three additional issues:

1. **A siloed case-by-case approach to enforcement, which creates confusion, rather than clarity**. While the EDPB has provided opinions and drafted clear guidelines on consent to feed into the discussion, it has never publicly taken a clear, unified stance on these models until the recent opinion. As a consequence, DPAs have acted differently and provided contradictory answers. The recent Meta Bundeskertellamt case shows another facet of this approach; while demonstrating how competition law can support data protection enforcement against Big Tech, it also indirectly created confusion around the legality of "pay or consent" models. In answer to a specific question asked by competition authorities regarding their competence to rule on a dominant company's compliance with the GDPR, the case specified "if necessary for an appropriate fee", words which were then interpreted by companies to mean that "pay or consent" could, in theory, be legal. However, given this was part of a narrow argument in a competition law context, this phrase should not be seen as the judiciary's definitive stance on data protection law, especially without any explanation on how to interpret it or how this could ever be compatible with the GDPR and human rights.
2. **Glaring gaps and disparities between Member States.** By approaching the questions for interpretation left out from the GDPR on a case-by-case, reactive, and selective basis, rather than a proactive and harmonising one, EU and national regulators have postponed addressing the underlying issue. This has further exacerbated the violation of the EU Charter and the GDPR, meaning that people in different Member States benefit from varying levels of human rights protections.
3. **Slow enforcement.** Legislators' lack of adequate response has been exacerbated by the slow enforcement of the GDPR that we have previously illustrated. This has allowed companies to continue with "business as usual", using the absence of clear-cut legal answers on the "pay or consent" models to disregard the Charter and GDPR's principles.

Before last year, the "pay or consent" model discussion was dormant, but the scandal ignited by Meta's policy shone a spotlight on the conflict between the digital advertising sector's economic foundations and people's fundamental rights and freedoms. This put pressure on DPAs to provide clear unified answers for all companies. In January 2024, Norway, Austria, and the Netherlands filed an urgent request for an EDPB Opinion, and three months later, the EDPB responded. However, this Opinion had a limited scope and was therefore only partially satisfactory. While taking positive steps towards a Charter-respecting interpretation on which to build, the Opinion raised some frustrations because of its unclear application to "large platforms" and the fact that dangerous outstanding gaps and backdoors could be misinterpreted. The EDPB is now expected to issue guidelines with a broader scope that will tackle the question on all fronts, not only in relation to Meta or to large platforms. If

done right, these could establish a strong foundation for the adequate enforcement of legally binding data protection standards and the EU Charter.

**EU regulators cannot afford to miss this opportunity to finally provide clear legal answers that will put people's rights first.**

# III. THE BOOM AND VARIETY OF "PAY OR CONSENT" MODELS

The EDPB Opinion raised concerns due to its narrow but unclear scope, leaving many uncertain about which companies were included in its scope. The world of advertising technology ("AdTech") is complex and diverse, going far beyond large online platforms. Understanding this ecosystem's history, operations, and power dynamics is critical to creating a comprehensive regulation fit for the digital age.

Legal scholar and professor on privacy, Julie Cohen, notes that behavioural advertising emerged from Big Tech platforms' need for a sustainable business model. According to Cohen, after entering the stock market following investment in their technologies, companies such as Google realised that, to keep growing at the same speed, they needed a stable and profitable source of income.[11] Enter: targeted advertising.

But even as the GDPR was entering into force in parallel, it became clear that it would be difficult for companies to argue that behavioural advertisement could be done without freely given consent, given its invasiveness. By then, however, Big Tech companies were already monopolies or "moligopolies", thanks to their behavioural advertising: and other companies fell quickly under the same system's thumb. Innovation stagnated and online businesses found that, in order to survive in the online space, they had no choice but to also adopt behavioural advertising models, which only reinforced the monopolies' power.

As a result, an online ecosystem was created where we saw some companies, such as Meta, using targeted ads with legitimate interest as their basis (TikTok also attempted this), some using targeted ads with real consent, some using targeted ads with "pay or consent" models (Meta and Der Standard newspaper), some using "pay or consent" models mixed up with other revenue models (e.g. freemium models), others using contextual advertisement, and some others using business models not involving targeted advertising.

As Cory Doctorow, journalist and author, has said: "*for systemic problems we need systemic solutions — not individual ones*." With this in mind, here are four things to consider when creating systemic solutions to address the proliferation of "pay or consent" models:

[11] Julie E. Cohen, Between Truth And Between Truth and Power: The Legal Constructions of Informational Capitalism, Oxford University Press (2019), page 41, 55.

1. Due to the lack of cohesive legal stance on "pay or consent" models, we see more and more companies finding new ways to implement such models. These include mixed "pay for your privacy" models that combine requests for consent for different purposes or payment for subscription for goods or services with payment for privacy in one pop-up window, or models using double paywall tricks (a cookie paywall for tracking followed by another paywall if the first is accepted).[12] These approaches all share a core idea: whether directly or indirectly, they remove people's agency by making refusal of consent conditional on payment. But the GDPR states that people must be able to give consent separately for different purposes.[13] **To ensure this issue will be addressed comprehensively, future actions must address *all* models, using methods able to address any type of "pay of consent" rationale.**

2. Given that Big Tech companies control the online ecosystem and considering the need to prevent further cementing of gatekeepers' ability to profit from data exploitation, all models that involve any form of "pay or consent" should be prohibited. According to the GDPR and other laws, **there are no exceptions for compliance with the law depending on the size of a company; there are only additional responsibilities.** While more effort and attention should be focused on the largest players profiting most from data exploitation, anyone using "pay or consent" is openly putting a price tag on human rights. We need to address the issue as a whole, with clear guidelines that will create an even playing field for small and medium-sized businesses.

3. These models are proliferating fast across a wide range of sectors, leading some companies to lobby for exemptions from GDPR rules. But such exceptions would not only perpetuate ongoing harms and fail to address root causes, but would not align with the GDPR, which does not allow for a differentiation depending on the business sector one operates in. News publishers that have been implementing "pay or consent" models argue that to survive in the Big Tech-dominated market, they need to engage in behavioural advertising, although this leads to further dependence on these monopolies. In fact, many alternatives do exist, like contextual advertising, and these offer more sustainable and independent financial support, challenging the narrative that behavioural ads are essential for survival. To ensure that no one can coerce people into a "pay and consent" scenario, **we must ensure there are no exceptions for any kind of business, from any sector.**

4. **Alternative business models that don't involve "pay or consent" or behavioural advertising do exist**. The EU should support models that do not rely on "selling" fundamental rights. Prohibiting "pay or consent" could help create a world where people have a real choice over their engagement with behavioural advertising, and where there are many other ways for businesses to earn revenue. Such an approach could help jumpstart innovation, and create a

[12] Presentation of Cristiana Santos at the Consent or Pay EDPS event, 11 July 2024.
[13] Recital 43 and Article 7(2) GDPR and 5 (1) b).

healthier, more sustainable, and competitive environment. By promoting alternative, legal and human-rights compliant models, where privacy is embedded by design, the EU can not only limit Big Tech's market dominance, but also create the desired competitive market.

# IV. GENERAL RECOMMENDATIONS

As outlined in the introduction, "pay or consent" models conflict with the EU Charter of Fundamental rights. Article 51(1) Charter of the EU, a legally binding instrument, states that the EU and its Member States have a duty to respect, observe, and promote all fundamental rights, including the right to privacy and data protection. The EDPB must provide clear guidelines that prioritise human rights over monopolistic interests, setting the stage for comprehensive, fundamental rights-centred enforcement across all legal frameworks. This is essential to uphold the GDPR's principles and to ensure that privacy and human rights remain central to EU policies, preventing the erosion of fundamental protections. All future actions taken to address "pay or consent" models will need to properly tackle related structural issues to deal with their illegality, and will need to address the ecosystem in which they operate. Tackling the symptoms will not be enough; only legal certainty over the core question will end this legal debate.

## RECOMMENDATIONS FOR THE EDPB

### 1 Clearly declare that binary "pay or consent" models breach the Charter of Fundamental Rights of the EU and render consent invalid, therefore breaching the GDPR

The EDPB Opinion on Pay or Consent recognises the incompatibility of "pay or consent" models with both the Charter of the EU and the GDPR, and reiterates that privacy cannot be treated as a commodity and is non-transactable. However, the Opinion frustratingly leaves too many back doors open to interpretation, weakening its objective and creating legal unclarity.

- **Specify regardless of scale**. The ban on "pay or consent" models should apply to all services, regardless of size. More precisely, the assessment criteria for valid consent developed by the EDPB should be able to address and uncover any illegal consent options, regardless of the size of the business. Extra guidance and enforcement effort should then reflect the impact of large and dominant platforms in aggravating their infringement of the GDPR (see recommendation six below).
- **Specify without differentiating between business sectors.** Consent should be free for all. The GDPR does not allow for differentiation or privileges based on the type of service or platform, and the EDPB Opinion also does not differentiate by sector. Moreover, human rights apply equally to everyone. With "pay or consent" models

spreading across every context and sector, exceptions could be misused and in any case, would only address symptoms, rather than the core issue.

- **Specify that offering alternative behavioural advertising options which process less data still breaches the GDPR**. Offering this type of alternative still involves behavioural advertising and the same "pay or consent" logic, forcing people to choose to either pay a lot, or a little less, for their rights, without addressing the underlying problem of a binary choice.

## 2 Mandate granular, people-friendly consent

- Granularity of consent is essential to fight "pay or consent" models at their core.[14] This helps to ensure that companies comply with their transparency obligations and that there is no misleading information, that consent is genuine, and that companies trying to escape any prohibition on "pay or consent" models have to divide privacy and goods, or uncover double paywalls. Granularity of consent can also help fight the use of "deceptive design patterns" that can affect users' privacy decisions, and which appear in 97 percent of websites and apps.
- To ensure that granularity criteria can be applied in a practical, people-friendly way, we suggest that the EDPB consults with experts to provide examples on how to frame granularity in a way that gives people agency, without creating extra burdens. We specifically encourage consultation with psychologists to reflect on factors that could encourage freedom of choice for people faced with more granular consent options.

## 3 Support and publicly map alternative, privacy-friendly business models

- As we have noted, alternative business models exist. By prohibiting "pay or consent" models companies will still be able to offer consent-friendly behavioural advertising that is transparent and compliant with the GDPR. The future we envision is one where people have agency, and other business models where people can choose and are aware of what happens are available.
- The EU, and in this context the EDPB, should support alternative business models by showcasing and supporting existing examples of privacy-friendly alternatives that do not undermine sustainable business revenue flows and which respect the EU Charter. This will help support and empower disadvantaged actors.
- Practically, the EDPB should suggest the following steps for businesses to choose their business model:

[14] EDPB Opinion on Pay or Consent, page 31.

- Firstly, check if revenue is truly needed;
- Secondly, assess the necessity of a model involving personal data, by building on existing research and by checking the availability of other business models;
- Thirdly, if the decision to include a behavioural advertising option is taken, ensure that consent complies with both the Charter and the GDPR, that all GDPR principles are respected, and that the prohibition on "pay or consent" is respected.

**4**

**Underline controllers' transparency obligations, the illegality of misleading advertisement and deceptive designs, and the incompatibility of these practices under consumer law**

- "Pay or consent" models lack transparency, and undermine user agency; 99 percent of people accept the binary choice without understanding its implications.[15] In addition, research shows that most websites employ deceptive designs that manipulate people's private decisions. Other research shows "that websites might continue to track users even when they pay the fee, constituting user deception." Transparency is crucial for valid consent under the GDPR, but users are often unaware of how their data is used. According to the Norwegian Consumer Council, "consumers are more or less powerless to prevent the harms that the system facilitates or makes possible."[16]
- The EDPB should emphasise the importance of transparency, integrating useful parts of consumer law, using existing examples and alternative options to guide companies and to support DPAs with enforcement. DPAs should be encouraged to directly refer to consumer law as supporting evidence in their cases.

## RECOMMENDATIONS FOR THE NEW EUROPEAN COMMISSION

**5**

**Complete and adopt a modernised ePrivacy Regulation to harmonise additional protection for people's privacy and their right not to be tracked**

- By harmonising the law to protect the privacy and confidentiality of electronic communications, the EU could increase people's protections from the harms

[15] See from Noyb (2023): "More than 99 percent of people decide against a payment when faced with a "privacy fee." *Noyb files GDPR complaint against Meta over "Pay or Okay"*.
[16] Forbrukerradet (The Consumer Counsel of Norway), Out of Control: How consumers are exploited by the online advertising industry, page 179.

mentioned in the introduction. Additional regulation would govern the use of tracking technologies that enable this surveillance ecosystem. The concept of consent and agency already present in the GDPR would thus be strengthened.

**6** **While using new competition powers under the DMA, closely cooperate and coordinate with the EDPB and consumer authorities**

- Big Tech companies are rolling out "pay or consent" models to maintain their data monopolies and potentially block privacy-friendly alternatives, stifling innovation. To confront these models and create a support system for smaller actors, the EU should use competition law boldly alongside the GDPR and the DMA, to challenge and topple Big Tech's dominance. In practice the Commission should continue to proactively use its powers as enforcer of the DMA and competition law to the fullest, to cement the EU Charter and to protect GDPR principles. To do so, it should closely cooperate with privacy watchdogs and consumer law authorities, as it did to develop its preliminary findings on Meta's "pay or consent" approach.

## GENERAL RECOMMENDATIONS FOR EU ENFORCEMENT AUTHORITIES

**7** **Cement the precedence of human rights**

- **Be proactive in your enforcement.** While this report focuses on "pay or consent" models for behavioural advertising, we underline that there is no place for "pay or consent" models for any commercial purpose that a company might claim. We are particularly worried, for instance, about the use of "pay or consent" for training AI; platforms such as X and Meta have tried to argue legitimate interest as a basis for scraping people's data in order to train their AI models. It is important to provide adequate and accurate explanations when banning "pay or consent" models to ensure the discourse is not revived with a view to new and emerging commercial purposes, such as AI training.
- **Unequivocally reject any threats to the foundational principles of the GDPR**. At this point in time, with privacy at a crossroads, it is important to proactively enforce, and reinforce, the principles of the GDPR and demonstrate how they should be respected in future conversations about "pay or consent". Even the EDPB has stressed that obtaining consent does not negate or in any way diminish the controller's obligations to observe the principles of processing enshrined in the GDPR.

# V. CONCLUSION

To conclude, "pay or consent" models are the perfect example of a GDPR enforcement test waiting in limbo for years on end. Privacy is at a critical juncture and we are at a crossroads; either we stand by the values on which the EU is based, or we start down a path to lowering human rights protections, one paved with exceptions and back doors.

The direction the EU takes on this issue will shape data protection for years to come. As the new European Commission's mandate begins, now is the moment to push back on industry narratives and make the promises of GDPR and a privacy-by-design future a reality, by addressing the issue at its core. All of our recommendations provide practical ideas for how this new enforcement framework could work, based on the legally binding instruments of the EU Charter and the GDPR.

We look forward to collaborating with the EU to reach a final consensus on this topic. We stand firm in our commitment to preserving the integrity of the GDPR and ensuring that individuals retain genuine control over their personal data, without coercion or discrimination and with respect for their fundamental rights.

**For more information, visit our page: https://www.accessnow.org/data-protection/**