Is Pay or Consent a choice under GDPR?

April 5, 2024

Offering an alternative between payment and advertising is not per se contrary to the freedom of consent under the GDPR

Recent European data protection decisions have reshaped the advertising landscape, prompting strategic choices between advertising and payment. Such alternative is now challenged by the freedom of consent requirement under GDPR. The ‘pay or OK’ debate requires a consistent articulation between consumer protection (contract law and fairness), competition (pricing) and privacy protection (individuals rights) rules. Since 2020, no EU DPA that has adopted a position on ‘paywalls’ has issued any general prohibition. Instead, they have established a list of criteria feeding case-by-case analysis. In July 2023, the ECJ pushed back a mere ban of ‘pay or OK’ models. Now, the much expected EDPB opinion to be issued this spring regarding the paywall proposed by Meta will be key. The threat of an outright ban on subscription-based models would jeopardize digital press and media who depend on personalized advertising revenues. All in all, same consent rules should apply to all service providers.

Executive summary

Advertising has long been the backbone of the media industry's economy, but the role of advertising in a world filled with information and services is being questioned. Recent European data protection decisions have reshaped the advertising landscape, raising questions about the balance between advertising and fundamental freedoms such as data protection, freedom of expression, assembly, and the right to conduct business.

Companies funded by advertising are increasingly turning to subscription-based models, such as *'paywalls*', to compensate for users who refuse consent for personal data collection for personalized advertising. In essence, subscription-based models are a means for digital businesses to sustain themselves and continue offering their services in a financially viable manner.

Digital press, media, and content publishers rely heavily on advertising for revenue. They have various costs to cover, including content, employee salaries, licenses, data hosting, infrastructure, and more. Without advertising and paywall options, these digital businesses would struggle financially, as contextualized or non-personalized advertising generates significantly lower revenue.

Running any business incurs costs, and the criticism of Meta's subscription-based model often revolves around the misconception that users are selling their privacy. In reality, paywalls provide a price for the service itself, not for user’s privacy. Notably, privacy isn't 'bought' in this model; users decide between (1) payment and access to the service that is compliant with data protection regulations, or (2) free access to the service that is still compliant with data protection regulations.

The idea that digital services should be free is unrealistic. No private business, regardless of its size, is required to provide its services for free. Even essential services like water, oil, gas, or electricity are provided for a fee because they involve resources that must be purchased and resold.

The rise of paywall alternatives in the digital landscape raises questions about user’s consent and freedom of choice. An analysis of these alternatives and their impact on user’s freedom of choice is crucial. In the subscription-based model, users have options. They can choose to pay for a service or consent to personalized advertising / advertising cookies for free access while still benefiting from all their data protection rights.

Consent plays a pivotal role in targeted advertising, given limitations of the use of other legal grounds. Users must have transparent choices and a clear understanding of terms of such consent and its alternative. While digital service providers typically determine prices, the validity of the "GDPR" consent of users is not linked to their ability to control pricing. What matters most is that users are fully informed about available options and the consequences of their choices, emphasizing transparency. To enhance user's freedom in the digital realm, it is essential to focus on improving user's comprehension of both personalized advertising consent and a paid subscription option, potentially through regulations ensuring clear, concise, and understandable presentation of terms, aligning with GDPR principles.

In the EU, the legality of subscription-based models remains uncertain and no clear regulation dealing with both data protection principles including the validity of user's consent as defined by GDPR, and online services offerings, labels paywalls as universally lawful or unlawful.

Following a legal challenge by industry associations especially press and media publishers, including GESTE[1], the Conseil d'État (French highest administrative court) ruled on June 19, 2020, that the CNIL couldn't impose a blanket ban on cookie walls. The court emphasized that obtaining free consent for data processing should be evaluated individually, in consideration of diverse situations and contexts.

As a result, the CNIL revised its cookies guidelines in September 2020, admitting that the validity of cookie walls or paywalls with regard to the freedom of consent requirement should be assessed on a case-by-case basis, combining the following criteria:

- Offering a fair alternative to cookies acceptance;
- Providing an equivalent service by the same provider;
- Setting a reasonable price for alternatives;
- Limiting cookie purposes in paywalls to justified ones.

The Danish, German, Italian, Spanish, UK DPAs have also acknowledged the potential legality of cookie walls, under similar conditions. Although not all European countries have expressed the same position, the current regulatory trend among the authorities that have issued comprehensive guidance on cookie walls / paywalls emphasizes a user-centric approach.

Instead of an outright ban on subscription-based models, such authorities are advocating for a careful, case-by-case analysis to ensure that users are aware of their choices and can make them freely and with informed consent. These are exact same criteria as those required under consumer protection laws, in particular regarding fair commercial practices. European privacy regulators should acknowledge the legitimacy of paywalls and advertising alternatives under applicable laws and provide concise guidelines paving the way for case-by-case decisions to harmonize the criteria ensuring the protection of user's privacy in subscription-based models, such as paywalls. A common regulatory approach would foster an environment where user's privacy and sustainable press and media economy coexist.

Unified EU guidance on paywalls resulting from close collaboration between data protection authorities (that would analyze the matter under privacy regulations) and competition/consumer authorities (that may intervene on pricing and marketing fairness subjects), would be necessary in order to stabilize the applicable framework ensuring the consistent regulation of business models vs. privacy considerations.

1 " *Groupement des éditeurs de services en ligne", a* French professional association of online publishers, including major French media groups.

The debates that are taking place within the 1st semester of 2024 within the EDPB regarding the paywall proposed by Meta will be key, as the threat of an outright ban on subscription-based models would jeopardize the future of the press and media in Europe, notwithstanding the necessary balance between consumer protection, competition and privacy protection rules. Indeed, the legal compliance of the subscription-based model also relies on pricing issues (competition law), transparency (consumer rights), and conditions to access and fund a service (contract law).

1. INTRODUCTION

Advertising has long been the bedrock of the media sector's economy. In today's world of intense competition between millions of sources of information and services, advertising and prioritization of contents in general are omnipresent across numerous channels, yet the general public does not deeply question the right to live in a world of media without advertising.

For the two past centuries, no press or media has ever existed without being substantially funded by advertising. Yet, in the privacy sphere, there is an ongoing conflict between those whose business models are dependent on advertising (publishers) and their non-paying users. This struggle centres around the question of whether users hold a right to access and use services free from both direct and indirect advertising or payment.

Indeed, recent stances and decisions taken by European data protection authorities and courts regarding online services offering a choice to users between subscription-based services, fee-based services and advertising-based services, lead to a reassessment of the role of advertising within the economic model of press, media and social platforms, and grant users more extensive rights than the rights they benefit from for other services. A critical examination of the interplay between these models and fundamental freedoms arising from the Charter of Fundamental Rights of the European Union (EU Charter) and the European Convention on Human Rights (ECHR), such as personal data protection, freedom of thought, expression, assembly, association, and – last but not least – the freedom to conduct a business, is paramount.

At the heart of the digital advertising debate is the protection of privacy and personal data, enshrined in Article 8 of the EU Charter. New advertising models, which often rely on user data to offer targeted content, must navigate complex requirements of data protection legislation resulting notably from the GDPR[2] and the ePrivacy Directive[3], notwithstanding Directives and Regulations protecting European consumers.

This exploration is not about respecting or not the fundamental rights of individuals to control their personal information and to protect their privacy – this is not even up for debate, – but to articulate them with other considerations leading to a comprehensive legal analysis.

Freedom of thought and expression, as guaranteed by both the EU Charter and the ECHR, comes into play when considering media services and platforms advertising models that might influence or limit access to shared information. The ability of individuals to freely express and receive information can be impacted by how digital platforms select or prioritize content based on popularity, interplays between individuals and advertising models. This raises questions about the potential of new models to inadvertently create echo chambers or filter bubbles.

While less directly related, the freedom of assembly and association is also relevant in a digital context where social media serve as spaces for community building and collective expression. The choice of content prioritization and advertising models can influence the nature of these digital spaces and the manner in which individuals can interact within them.

The freedom to conduct a business, as provided under Article 16 of the EU Charter and recognized in France as a principle of constitutional value by the "*Conseil Constitutionnel*", is crucial when considering the rights of digital platforms to adopt various advertising and revenue models. This freedom must be balanced against fundamental rights of individuals, ensuring that:

- business practices do not encroach upon the privacy and freedoms of users;

---

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**").

3 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("**ePrivacy Directive**").

- privacy rights do not plainly prohibit the provision of and access to free media.

Lastly, Article 54 of the EU Charter, which prohibits the abuse of rights conferred by the EU Charter, serves as a critical lens through which to view these new advertising models. This provision ensures that the exercise of rights by one party does not disproportionately infringe upon the rights of others, a principle that is highly relevant in the context of targeted advertising and user privacy.

The interplay between these fundamental rights and freedoms, with interests that may be competing depending on the context, is fully visible in the matter of subscription models implementation: freedom of expression between users vs. protection of their personal data collected in this context vs. the freedom of business operators, which should be able to decide to provide a service or not, and to determine its cost and price.

The outcome of this debate suggests an implicit ranking of rights and fundamental freedoms, with data protection on top of an undeclared and undebated hierarchy of norms. This perspective is influenced by the fact that when a business entity implements payment for an online service - *e.g.* a subscription model - it shifts from a previously free use model that all the current users have been used to since the introduction of such online service.

This standard free use model, in the user's mind, implied, completely erroneously, that maintaining the service incurs no costs. However, in the meanwhile the service has always been financed by revenues from targeted advertising, often practically invisible to users in the absence of a fee alternative. Revenues from non-targeted advertising are generally 70% lower than revenues from targeted (and in particular cookie-based) advertising. Therefore, contextualised or non-personalized advertisement alone does not provide any viable financial alternative for online service providers, especially press and media who may depend on advertising revenues for more than 90%.

The issue at hand is to:

- determine the true nature of these subscription models,
- while taking into account the current position of privacy regulators and courts, establish whether (and if so, how) the applicable law and an alignment between conflicting fundamental rights and basic economic principles might influence a private entity's choice of an economic model, and
- ascertain the actual extent of users' rights.

2. SUBSCRIPTION MODELS

2.1 Rationale for subscription models and examples

"Paywalls" represent an approach that is being increasingly used by companies that are wholly or partly financed by advertising revenue. By using paywalls, such businesses can compensate for any revenue lost because of the visitors not providing their consent to the collection of their personal data for advertising purposes (via cookies or other trackers, for simplicity, we only use the term "cookies" in the present article).

There is an important difference between a "cookie wall" in *stricto sensu* and a paywall:

- A strict "*cookie wall*" mechanism prohibits any access to an online service unless users consent to advertising cookies, without any alternative offered;

- A "*paywall*" offers the user an alternative between accepting advertising cookies and accessing a service free of charge, or paying for a service without any advertising resulting from cookies.

In the paywall model, the user is offered various options for accessing the content or services. The classic paywall model usually offers two main alternative paths (cookies or payment).

Users can therefore decide at their own discretion whether they are ready to pay money for an online service, or use it free of charge by giving their consent to advertising resulting from cookies, **all the while, in the case of both options, being protected under data protection principles that the service provider continues to comply with**: transparency, legitimate purpose of processing, proportionality and minimization, right of access, right of deletion, data retention limitations, etc.

The payment alternative offered to the user allows him/her to access the service without accepting the use of his/her data for targeted advertising purposes. **Free access alternative requires the user to consent to targeted cookie-based advertising, but both the consent and the cookies data processing for targeted advertising purposes still have to comply with applicable data protection regulations**.

It is important to strongly highlight this point: in a paywall model, the privacy of the user is not "bought". The alternative that is proposed to the user is not (and never can be)between:

- **Payment for provider's compliance with data protection regulations, and**
- **Free access for accepting provider's non-compliance with data protection regulations.**

The provider obviously has to comply with all data protection regulations, whether it uses advertising cookies, or accepts a subscription payment.

The paywall model takes into account both the user's interest in using the online service without tracking or advertising and the provider's economic interest in not having to provide its content and services free of charge.

Paywalls are a way to:

- empower individuals to make free and informed decisions about the use of their data, and
- allow companies to finance online content and services, taking into account part of the users whose data would not be used for targeted advertising and would therefore not contribute to the company's revenues.

2.2 Meta's case – regulatory focus

Right before the entry into force of the GDPR and in order to comply with it, Meta has modified the Terms of Service for its Facebook and Instagram users by introducing some mandatory information elements. As before, Meta relied on the legal basis of "contractual necessity" for most of its processing activities.

Users were thus asked to accept new updated Terms of Services to access their Facebook and Instagram accounts; otherwise, the services would not be available to them. Meta considered that such acceptance of the Terms of Services, that included acceptance of behavioural advertising, would be sufficient to support the application of the contractual legal basis under the GDPR.

On 25 May 2018, NOYB[4] filed two complaints to Ireland's Data Protection Commission ("**IE DPC**"), IE DPC being the lead supervising authority for Meta. Both complaints argued that the forced acceptance of the Terms of Use constituted a forced and thus invalid consent.

The IE DPC commenced two inquiries and has found in its draft decision, after more than 3 years of investigations, that Meta was in breach of several GDPR obligations, and in particular the

[4] None of Your Business, organization founded by Max Schrems, focusing on advocating for data protection and privacy rights under the GDPR.

transparency requirement, claiming that the contractual legal basis had not been clearly identified. The IE DPC proposed to sanction Meta and to impose GDPR fines on this basis.

As to the "*forced consent*" criticism, IE DPC had initially taken the position that Meta did not force the users to consent, and more generally, that Meta was not required to rely on consent for its data processing activities, including for behavioural advertising purposes. IE DPC was ready to accept the applicability of the contractual legal basis as argued by Meta.

Pursuant to Article 60 of the GDPR, the IE DPC submitted the draft decisions to Concerned Supervisory Authorities in the EU ("**CSA**").

Some of the CSA took the stand that Meta should not be permitted to rely on the contract as a legal basis since the delivery of personalized advertising would not be necessary to perform the core elements of the service. The IE DPC disagreed with this strict approach, stating that the Facebook and Instagram services were based on the provision of a personalized service that necessarily includes personalized or behavioural advertising.

After failing to reach a consensus, the IE DPC referred the decision to EDPB who imposed its own binding decisions (decisions No. 3/2022 and No. 4/2022 of 5 December 2022). The EDPB decided that Meta inappropriately relied on contract as a legal basis to process personal data in the context of Facebook's and Instagram's Terms of Service for the purpose of behavioural advertising, as this was not a core element of the provided services. Consequently, the EDPB considered that Meta lacked a legal basis for this processing, which therefore was deemed unlawful under the GDPR.

EDPB instructed the IE DPC to amend its draft decision in order to include Meta's infringement of Art. 6(1) GDPR (processing without a legal basis), and to increase the amount and number of imposed fines. On 4 January 2023, IE DPC announced:

- the conclusion of two inquiries against Meta[5] ;
- the decision according to which Meta cannot process personal data for the purposes of behavioural advertising relying on a contract as a legal basis; and
- the decision to issue a €390 million fine (total).

Meta was ordered to bring these behavioural advertising processing activities into compliance with Article 6(1) GDPR within three months.

On 4 July 2023, the Grand Chamber of the Court of Justice of the European Union ("**CJEU**") handed down its judgment in Case C-252/21, Facebook Inc. and Others v Bundeskartellamt. In considering Meta's processing of user data collected off- Facebook (*i.e.* data collected from other Meta services and third-party sites, as opposed to user data collected on Facebook), this judgment held, subject to final factual determinations to be decided by the national court, that:

- Meta's use of "contractual necessity" as their lawful basis for the processing of EU user's personal data for behavioural advertising was in violation of GDPR;
- Meta could also not rely on legitimate interests legal basis for processing of personal data for the purposes of personalized advertising, as:
    - users cannot reasonably expect their personal to be used for personalized advertising without their consent,
    - therefore, such legitimate interest of Meta to use personalized advertising to fund its activities would be overridden by individuals' fundamental rights and interests; and

5 IN-18-5-5 dated 31 December 2022 and IN-18-5-7 dated 31 December 2022

- o the processing at issue is particularly extensive since it relates to potentially unlimited data and has a significant impact on the user, which may give rise to the feeling that his or her private life is being continuously monitored.

Therefore, as a result, both the IE DPC and the CJEU, with the involvement of the EDPB, have definitively ruled out the use of contractual legal basis for Meta's behavioural advertising activities.

The use of Meta's legitimate interests for such behavioural advertising processing has also been challenged by the CJEU as outlined above, which made reliance on legitimate interests a legally insecure option for behavioural advertising processing.

CJEU has further stated that users must be free to refuse individually to give their consent to particular data processing operations (not necessary for the performance of the contract), without being obliged to refrain entirely from using the service offered by Meta.

According to CJEU, this means that these users should be offered an equivalent alternative not accompanied by such data processing operations, if necessary for an appropriate fee.

This has left consent (and associated paywall) as the only available legally secure alternative for behavioural advertising, for Meta as well as any other actor using behavioural advertising to fund media and publishing services.

In this context, Meta has introduced a paywall for its Facebook and Instagram services offering its users an alternative between:

- Consent to cookies and to personalized advertising processing activities, or
- Subscribe to an ad-free version of the services for 9.99 (desktop) / 12.99 (mobile) EUR / month.

Meta's paywall system has faced criticism on several fronts:

- **Economic accessibility and content access / quality**: Critics highlight that paywalls might exclude individuals who cannot afford subscriptions or one-time fees, creating disparities in access to information based on economic status. The paywall could also lead to prioritizing content that appeals to paying subscribers, and restrict access to information, making it exclusive to those who can afford to pay. However, this argument only works if Meta offers different (non-ads) content to subscribed and "free" users, which is not the case;
- **Impact on media and content publishers**: There are concerns about how revenue sharing is handled between Meta and content creators. Some worry that the terms might not be favourable to smaller creators or publishers, affecting their ability to monetize their content fairly. However, it is projected that the vast majority of revenue for Meta would still come from targeted advertising and not subscriptions, which would mean that the paywalls wouldn't affect the existing balance of interests;
- **Data privacy and freedom of consent**: NOYB, among other critics, consider that the proposed paywall system does not allow users to give a free consent. Their consent to the "free" option is allegedly invalid with regard to the GDPR's requirements.

The issue of the user's freedom of choice and its validity under the GDPR is central to any paywall system and requires to differentiate between offering an alternative or granting a discretionary right not to pay a service.

3. USER'S FREEDOM OF CHOICE

The issue of a user's freedom of choice appears as the major topic in the field of targeted advertising.

This subject relates to the question of the perimeter of the user's freedom of choice: (i) whether, (ii) at what point and (iii) under what conditions a user has the fundamental right to express consent to processing of his/her personal data when such processing ensures some of the functionalities of a service, and what the influence of the fundamental right to privacy protection can be on the economic activities of a company in the digital economy. Ultimately, it involves discerning the line that separates giving consent to targeted advertising used within a service from actively demanding to benefit from a service.

As a general comment, neither profiling (as referred to in Article 22 of GDPR) nor personalized advertising that does not use any cookies, are subject *per se* to any particular consent requirement under GDPR. Cookie-less advertising can be (and is in most cases, especially for e-commerce services) based on the data controller's legitimate interests, subject of course to the user's comprehensive and complete prior information, right to object (generally from the moment of collection of personal data), as well as the balance between the rights of users and such legitimate interests.

The question of user's consent and of freedom of such consent arises in its full glory for cookie-based targeted/behavioural advertising. Indeed, such consent is not imposed by GDPR *per se*, but by the ePrivacy Directive requirements (as outlined below). Once the requirement for a user's consent is established (under ePrivacy), it is then interpreted under GDPR principles and definitions, including the requirement of freedom of consent (and its conditions).

However, Meta's case analysed in point 2(b) above concerned personalized advertising in general and not necessarily cookie-based advertising. While for smaller players, consent requirement would generally be only applicable to advertising cookies and not to any "cookie-less" profiling activities, consequences of Meta's case may change this *status quo*.

3.1 **The legal grounds for personalized advertising: is consent the only way?**

Personalized advertising operates within a complex regulatory framework influenced by the GDPR, the ePrivacy Directive, the guidelines from the EDPB and data protection authorities, as well as consumer and competition laws, and eventually major new regulations targeting digital sector such as the DSA[6], the Digital Market Act[7] or the emerging Data Act[8], notwithstanding the Artificial Intelligence Act.

This complex legal framework, sometimes pertaining to areas of law that are relatively distant, should prompt an examination of the legal basis on which an economic operator is entitled to carry out specific operations such as personalized advertising. In the end, the key inquiry is whether the consent of a user serves as the only available legal ground for engaging in personalized advertising initiatives.

(a) **Legal bases deriving from data protection laws**

Article 6 of the GDPR outlines several legal bases for the lawful processing of personal data. The most relevant for personalized advertising could be (i) performance of a contract, (ii) legitimate interests, or (iii) user consent.

(i) Performance of a contract under Article 6(1)(b) GDPR

Evaluating the legitimacy of 'contract' as a legal basis for personalized advertising presents a nuanced perspective. Article 6(1)(b) of the GDPR allows personal data processing if it is "*necessary*

---

6 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC ("**DSA**").

7 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 ("**DMA**").

8 Proposal for a Regulation the European Parliament and of the Council on harmonised rules on fair access to and use of data ("**Data Act**").

for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract".

This requires that the processing be objectively indispensable for a purpose integral to the contractual obligations intended for the data subject. It is crucial for the data controller to demonstrate how the main subject matter of the contract cannot be fulfilled without such processing of personal data.

For personalized advertising to legitimately rely on the contract as a legal basis under the GDPR, it would require for the prioritization and display of advertising/personalized content to be an integral and necessary component of the service provided under the contract, and not merely a convenient or profitable addition. This requirement is meant to ensure that the processing aligns with the user's reasonable privacy expectations when they agree to the terms of service, respecting the principle of fairness and transparency enshrined in the GDPR.

As explained above, the EDPB and various national data protection authorities have stated that the mere provision of a service, such as a digital platform, does not automatically make advertising activities necessary for contract performance. This issue followed two complaints lodged by NOYB with respect to the Terms of Service and Privacy Policy of Meta, which had initially stipulated the use of the contract as legal basis for the processing of personal data in the context of personalized advertising.

The IE DPC, serving as the lead authority, initiated a cooperation mechanism. This process led to several interpretations being raised by various authorities, especially about the legal basis in question, leading to the two decisions taken by the EDPB on the November 5 2022[9]. Finally, on December 31, 2022, the IE DPC issued two decisions stating that Meta could not base its behavioural advertising processing on the contract-based legal ground.[10] (for more details, see point 2(b) above).

However, this approach raises doubts as to whether it should have the effect of totally excluding the legal basis of the contract for targeted advertising, or whether it is a solution specific to the circumstances of the case and Meta's specific position on the market.

On July 4 2023[11], the CJEU ruled that the applicability of Article 6(1)(b) of the GDPR should also be assessed in the context of each service offered separately if the contract consists of multiple independent services or elements. While personalization of content may be useful to a user, enabling him/her to view content largely aligned with his/her interests, it is not necessarily indispensable for providing the services of an online social network.

According to the CJEU, an equivalent alternative service that does not involve such personalization could be offered, thus demonstrating that personalization is not objectively indispensable for the integral purpose of those services.

Therefore, based on the current position of the CJEU and the data protection authorities, data processing carried out in the context of personalized advertising cannot be based on the performance of a contract as it is not objectively required for the provision of online services.

(ii) ***Legitimate Interest under (Article 6(1)(f)) GDPR***

---

9 EDPPB Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service, adopted on 5 December 2022; EDPB Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service adopted on 5 December 2022.

10 Data Protection Commission, Facebook service decision, IN-18-5-5, dated 31 December 2022; Instagram service decision, IN-18-5-7 dated 31 December 2022.

11 CJEU, case C-252/21, Facebook Inc. and Others v Bundeskartellamt, adopted on 4 July 2023.

The legal basis of “legitimate interest” allows for data processing if it is necessary for the purposes of legitimate interests pursued by the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

The use of legitimate interests for personalized advertising requires a threefold assessment:

- the pursuit of a legitimate interest demonstrated by the data controller (or a third party),
- the necessity of processing of personal data for these legitimate interests, and
- the demonstration that these legitimate interests do not override the fundamental rights and freedoms of the data subject.

This requires a balancing of interests, where the data controller must ascertain whether the legitimate interests pursued by data processing cannot be as effectively achieved by less intrusive means, especially considering the rights to privacy and data protection of individuals.

Considering the most recent case law from the CJEU[12] (which related to the processing of the non-Facebook data by Meta), it appears that the use of the legal basis of legitimate interests in the context of personalized advertising may be challenged and considered unacceptable.

Indeed, although according to Recital 47 of the GDPR, the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest, in Meta’s case, personalized advertising was unable to benefit from this legal basis. This case law would inevitably affect all the other service providers who currently largely rely on the legitimate interests legal basis for personalized advertising (that is not based on advertising cookies).

In the abovementioned case, the CJEU emphasized that the legitimate interests pursued must be balanced against the rights and freedoms of the data subject, taking into account the specific circumstances of each case. This balancing act involves considering whether the legitimate data processing interests pursued cannot reasonably be achieved by other, less intrusive means. Importantly, the rights to privacy and the protection of personal data, as guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, play a pivotal role in this assessment.

For personalized advertising, this means that the data controller must demonstrate (1) the existence of a legitimate interest in processing the data for advertising purposes, (2) the necessity of processing to achieve this legitimate interest, and (3) the balance assessment according to which this interest is not overridden by the rights and interests of the individuals whose data is being processed.

In determining whether the processing is necessary for the legitimate interest, the requirements of proportionality and subsidiarity must be assessed:

- the impact on the data subject's interests should be proportionate to the processing purposes, and
- it should not be reasonably possible to achieve the pursued purposes by means that are less detrimental to the data subject[13].

According to the CJEU (at least in the Meta’s off-Facebook data case), the inherent intrusiveness of personalized advertising, coupled with the personal nature of the data involved, often tips the

12 CJEU, case C-252/21, Facebook Inc. and Others v Bundeskartellamt, adopted on 4 July 2023.

13 Amsterdam District Court, Private law division, Case number / docket number: C/13/683377 / HA ZA 20-468, Judgment of 15 March 2023, DATA PRIVACY STICHTING / FACEBOOK NETHERLANDS B.V, META PLATFORMS INC., META PLATFORMS IRELAND LTD.

balance in favour of protecting individual rights and freedoms, making it challenging to justify personalized advertising on the basis of legitimate interests.

National courts will have to draw their own conclusions following this recent CJEU case law.

(iii) ***Consent under Article 6(1)(a) GDPR***

As outlined above, with the legal basis of the contract ruled out by the recent CJUE and data protection regulators' decisions, and with the legal basis of legitimate interests becoming more challenging and less legally secure, personalized advertising activities have to turn to the consent legal basis.

According to GDPR, consent must be freely given, specific, informed, and unambiguous to be valid. In the context of personalized advertising, this means users must actively opt-in for the use of their personal data for personalized advertising, for example for the recording or reading of advertising cookies in their terminal device. The GDPR's high standard for consent has significant implications for advertisers, as it necessitates clear and direct communication with users about why and how their data is used.

But in the context of subscription models and online services, there might be a confusion between:

- Profiling / personalized advertising "cookie-less" activities that are not, as a general rule, subject to consent;
- Specific profiling / personalized advertising "cookie-less" activities that might in certain circumstances be subject to consent where legitimate interests legal basis cannot be used – as was decided by the CJEU in July 2023 for Meta's personalized advertising regarding non-Facebook data; and
- Cookie-based personalized advertising activities that are always subject to consent, but this consent legal basis is requirement stems from the ePrivacy Directive technical requirements and not from GDPR. The GDPR intervenes *a posteriori*, to define the way such consent must be given.

The ePrivacy Directive as amended in 2009 (nine years before the enforcement of the GDPR), specifically addresses privacy issues in electronic communications, and is deemed complementing the GDPR. User explicit consent is required for the use of cookies or similar tracking technologies used in targeted advertising. Since the GDPR was enacted to replace the former Directive 95/46 it succeeded, the definition of consent applicable to ePrivacy Directive is that by reference to the GDPR.

In France, the French data protection authority ('**CNIL**') has further clarified the requirements on how to collect user consent for cookies and trackers. Its guidelines delineate the nature of consent that must be obtained for using personal data in cookie-based advertising. According to CNIL, consent must be clear, unambiguous, and easily retractable, ensuring that users maintain control over their personal data. This guidance is significant for advertisers and businesses as it sets clear expectations and standards for lawful data processing in cookie-based advertising, ensuring compliance with the broader EU regulations.

But the ePrivacy Directive establishes consent as a requirement for storing/accessing of information (whether containing personal data or not) in the terminal equipment of a user. This consent requirement has not been introduced as a legal basis for such processing, but as a mandatory requirement for storing/accessing information on the user's terminal equipment.

Afterwards, the regulators have considered that this "ePrivacy" consent should be interpreted under the consent conditions as provided by GDPR, this virtually transforming this out-of-GDPR consent requirement into a consent legal basis.

Be that as it may, the consent requirement for cookie-based personalized advertising has been unanimously accepted by the EU data protection authorities since the adoption of the GDPR.

However, the requirement of consent to **any personalized advertising processing, even where it does not involve cookies**, is new and may have heavy repercussions on all of the online services providers.With the impossibility to invoke contractual legal basis and a great uncertainty to invoke legitimate interests legal basis, such actors may be compelled to turn to the consent legal basis.

It remains unclear how such consent requirement can be imposed by regulators / case law where it is not imposed by the GDPR (the data in question is not sensitive) nor any other regulation (in the absence of cookies/trackers, ePrivacy consent requirement is not applicable for personalized advertising). Furthermore, even the right to object to profiling provided under Article 22 of GDPR would not apply to personalized advertising as it does not produce any legal or similarly significant effects concerning the data subjects.

(b) **Legal bases deriving from the EU digital legislations**

The European Commission's aims concerning the legal framework governing personal and non-personal data often suggest additional outlooks, which might act as precursors to forthcoming legislative endeavours in this domain.

For instance, the Digital Market Act, that introduces additional regulatory dimensions, focusing on the practices of major digital platforms that often dominate the targeted advertising landscape provides that :

"*Gatekeepers often directly collect personal data of end users for the purpose of providing online advertising services when end users use third-party websites and software applications.* […] *To ensure that gatekeepers do not unfairly undermine the contestability of core platform services, gatekeepers should enable end users to freely choose to opt-in to such data processing and sign-in practices by offering a less personalised but equivalent alternative, and without making the use of the core platform service or certain functionalities thereof conditional upon the end user's consent. This should be without prejudice to the gatekeeper processing personal data or signing in end users to a service, relying on the legal basis under Article 6(1), points (c), (d) and (e), of Regulation (EU) 2016/679, but not on Article 6(1), points (b) and (f) of that Regulation.*"[14]

This echoes the aforementioned CJEU ruling, where the judges found that:

"*Thus, those users must be free to refuse individually, in the context of the contractual process, to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations*".[15]

Hence, considering the limitations on using contract and legitimate interest as legal bases, **what alternatives are left for online service providers relying on personalized advertising?** Consent emerges as the sole acceptable option. Yet, insights from the DMA and the CJEU indicate that this impasse concerning legal bases significantly influences how services are rendered.

Ultimately, this situation bears profound implications on the user choice and freedom in the digital landscape.

---

14 Digital Market Act, Recital 36.

15 CJEU, case C-252/21, Facebook Inc. and Others v Bundeskartellamt, adopted on 4 July 2023, point 150.

3.2 The impact of the user's freedom to contract

(a) The role of user consent and price determination

Given the limitations on using "performance of a contract" and "legitimate interest," consent emerges as the main feasible option for legal data processing in personalized advertising. This has significant implications for user choice and freedom in the digital landscape, as service providers must navigate these legal complexities while offering clear and transparent options to users.

It is a widely accepted norm that it is the seller, not the client, who determines the prices of services or products. This dynamic is also prevalent in the digital realm, where any media and content publisher sets the terms and pricing for their services. This raises a pertinent question: Does the user have a say in the pricing of a service for their consent to be considered free? Let's explore this question in the context of contractual freedom and French contract law.

In contract law, consent must be free and informed. This implies a clear understanding of the terms of the contract, but does not necessarily require that the customer have discretionary control over price setting. In most economic sectors, consumers accept prices set by sellers, which is considered standard and legitimate business practice.

In the digital domain, users are often presented with binary options: accept the service with predefined conditions or reject it. While this may seem to restrict contractual freedom, it's important to recognize that this dynamic is not unique to the digital world. In almost all economic sectors, consumers face similar choices without the opportunity to negotiate prices or contractual terms, since such issues are not governed by individual and discretionary choices, but by public policy of consumer protection and competition authorities and courts, which define and sanction unfair commercial practices. In any sector, consumer’s power to negotiate prices is generally reduced or may even be non-existent (e.g. in a supermarket, an individual would have a choice to buy a carton of milk for a fixed price or to not buy it at all, no negotiation would be permissible). The consumer protection authorities and consumer protection legislation provide sufficient protection measures for such day-to-day power balance to be acceptable.

Regarding the subscription models, the fundamental question, therefore, is whether the alternative offer to pay for a service and avoid personalized advertising constitutes a real and informed choice for the user.

Subject to control of competition / consumer protection authorities that may control excessive or abusive prices, the fact that users cannot determine or negotiate the subscription price does not necessarily limit the freedom of their consent. However, it is crucial that users are fully informed and understand the conditions they are consenting to, respecting the principle of transparency.

The economic models of digital services, like those of Meta, are based on pricing structures set by the company. This reflects an economic reality where businesses are free to determine their prices. Moreover, freedom to conduct business is one of the highly recognized fundamental rights in Europe. For the users' consent to be considered free, it is more important that they have a clear understanding of the available options and the implications of their choices rather than being able to negotiate the price.

To enhance user’s consent freedom in the digital space, a more relevant focus would be on improving the user's understanding of terms and conditions of their consent, what it implies and what processing operations are involved, rather than on the ability to negotiate price or structuring of business models.

For subscription models specifically, this could involve regulations ensuring that both the terms of subscription which is offered as an alternative to consent to personalized advertising, and the conditions and scope of consent for personalized advertising, are presented in a clear, concise, and understandable manner – not specifically under the GDPR. The emphasis should be on

information and transparency to ensure that consent is absolutely free and informed, rather than on the ability to negotiate the price.

(b) **Price requirement does not invalidate freedom of consent**

According to recital 43 of GDPR, consent cannot be used as a legal basis where there is a "*clear imbalance*" between the controller and the data subject. Such situations of "*imbalance*" of powers between a data controller and an individual are assessed on a case by case basis, but some typical cases tend to automatically fall under this defect in consent, notably relationships between a citizen and a public authority, and between employee and employer[16].

The threshold for considering consent as invalid under recital 43 is quite high and includes such extreme criteria as "*deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent*."[17]

In this context, it is quite evident that if a service provider simply offers an alternative between (1) consent to targeted advertising, and (2) payment of appropriate fee to access the service free from targeted advertising, there is no clear imbalance that would prevent the data controller from considering consent as valid and freely given.

The EDPB further acknowledged that freedom of consent is not impeded by a simple fact that no equivalent service is provided by any other service providers, because "*freedom of choice would be made dependent on what other market players do*" and it would "*imply an obligation for controllers to monitor market developments to ensure the continued validity of consent*".[18]

The abovementioned recital 43 of GDPR does not mention absence of service alternatives from the competitors as a factor that would create an "*imbalance*" of powers and invalidate data subject's consent. This is not an oversight: legislator explicitly rejected the proposal to invalidate consent "*if the data subject cannot reasonably obtain equivalent services from another source without consent*."[19]

In other words, dominant position of a market player that offers a fee-based alternative to consent does not in itself qualify as a situation of "*imbalance*" that would invalidate consent.

Under the Data Protection Directive[20] case law, the CJEU invalidated consent as not freely given only in one case that represented financial side of consent as extreme economic duress: where the receipt of state aid that made up 30% to 70% of the beneficiaries' income was tied to the publication of certain details of the beneficiaries and the sums received[21].

No reasonable fee-based alternative that may be offered by online service providers in a pay or consent model could ever constitute a case of such financial importance as to invalidate user's consent, given current criteria of "*imbalance*" and freedom of consent.

In any case, for pay or consent mechanisms, the legal basis of consent has been designated by data protection authorities and by the CJEU, as the primary applicable legal basis, after having deeply scrutinized and rejected contractual necessity and restricted the scope for reliance on legitimate interests. By doing so, neither the DPAs nor the EDPB nor the CJEU entertained the

---

16 EDPB Consent Guidelines, paras. 16 et seq.

17 EDPB Consent Guidelines, para. 24.

18 EDPB Consent Guidelines, para. 38.

19 Note of 17 February 2015, Document 14707/3/14 REV 3, p. 3.

20 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

21 The CJEU itself did not explicitly address the argument that the applicants consented to the publication and could have chosen to avoid it by forgoing the aid, but Advocate General Sharpston rejected it: Opinion of Advocate General Sharpston, *Schecke*, C-92/09, para. 82

idea that the legal basis they deemed applicable would in practice be inapplicable solely on the grounds that a payment would imbalance the balance of powers and freedom of consent.

(c) Is a right effective only when it is exercised?

The rate of consent does not determine the effectiveness of the right to consent.

When a right is available, the fact that it is not exercised, has never justified waiving the protection offered by this right. In the context of mechanisms subject to the right to object and provided for by the GDPR and the ePrivacy Directive, it has never been envisaged to abandon the exercise of the right to object on the grounds that it was very little exercised.

For example, when it comes to email marketing, the right to object must be offered to individuals at two times: (i) when the email address is collected, and (ii) each time a marketing email is sent. It has never occurred to the regulator to carry out surveys on rates of the exercise of the right to object, and conclude that this right was not respected simply because the right itself was not exercised.

The same applies to the right of access. We have never seen a regulator put in question the usefulness or validity of a right of access on the basis of the number of individuals exercising it. In this example, we can estimate that less than 1% of individuals exercise their right of access, and that less than one person in 10,000 exercises it several times, and almost none exercises it systematically. Does this mean that access rights are systematically violated by companies because individuals do not exercise them often?

Consequently, any speculation that might be drawn from the rate of consent to estimate that individuals' rights are being violated because individuals give their consent too often, is based on a double cognitive bias.

Firstly, it suggests that the number of individuals who prefer a paid solution to an advertising solution should be 50/50. But which individuals would prefer to pay for ad-free version of a service? Only those for whom an advertising insertion constitutes such an aggression, intrusion or distortion of service that they prefer to pay rather than have advertising spoil their use of a service.

In a context where online services are accessible to everyone free of charge, except for high-value-added services for which some individuals are prepared to pay, the choice to pay is bound to be proportionally very rare. This does not mean that the alternative offered to individuals is unfair.

Secondly, this question of consent rate constitutes, in itself, a cognitive bias. Indeed, the very fact that a service is accessible via two alternative financing methods, either paid or via advertising, constitutes the very essence of the freedom of choice offered to individuals. Of the 100% of individuals who are offered the alternative, 100% have the ability to make a choice.

Whilst the reality of a choice can be summed up as a preference between advertising and spending one's money, this does not mean that this choice does not exist, and that this alternative does not have the characteristics of valid consent.

(d) Understanding the pay or consent alternative

In today's digital environment, the introduction of paywall alternatives by media and platform publishers poses a complex challenge regarding consent and user choice freedom. Analysing the nature of these alternatives and their impact on users' perception of choice freedom is crucial to understand their legitimacy.

The paywall alternative, often presented as an ad-free (or personalized ad-free) service, theoretically offers a broader choice to users. However, this option must be evaluated in terms of financial accessibility and value perception. Otherwise, if not all users have the financial means to

choose the paid option, or if such option is perceived not as an added value but as a necessity to avoid a negative experience, then the freedom of choice might be put into question.

In a context where the free alternative is saturated with advertising, users might feel a subtle pressure to opt for the paid version. This pressure can influence the freedom of their consent. The way options are presented is crucial: if the paid option is perceived as the only path to an optimal user experience, it could bias the choice and call into question the freedom of consent.

The GDPR demands that consent be given freely and in full transparency. In this context, the paywall alternative must be evaluated to determine if it truly is without constraint or with an acceptable constraint. Users need to be fully informed about the implications of their choice, both in terms of privacy and user experience.

In civil law, the freedom of consent is fundamental. If users are turning towards the paid option primarily to avoid the free version's drawbacks, this raises questions about the true freedom of their choice. Conversely, if the users are choosing the free version because the paid option is too expensive or is not at least equivalent to the content offered under the free version, the freedom of consent may also be challenged. Therefore, the conditions offered by media and content publishers must be fair and reasonable to respect the principle of free consent.

Digital platforms have the responsibility to ensure that both the free and the paid options offer at least an equivalent service in terms of content and the user experience. Concurrently, users should have the right to choose in a framework where their freedom is not compromised by pressure or manipulation tactics. This freedom of choice should be supported by comprehensive and transparent information.

This will enable a truly informed and free choice, in line with GDPR requirements and civil law principles. To this extent, the implementation of alternative paid solutions, upon closer examination, is not in violation of the applicable legal statutes.

Nevertheless, this viewpoint may diverge from the approach embraced by some regulatory entities, notably the data protection authorities.

4. A CRITICAL ANALYSIS OF REGULATOR'S POSITIONS AND PRACTISES

The EDPB's recent guidelines on tracking mechanisms, while providing clarity on tracking techniques under the ePrivacy Directive, fall short in addressing the burgeoning issue of paywalls.

Despite their legal permissibility under the current legal framework, there seems to be an implicit stance against paywalls taken by some of the regulators and data protection authorities, without any clear legal argumentation. This position appears to stem from several factors:

- some EU data protection authorities simply repeat the EDPB guidance according to which cookie walls are prohibited. Such ban should not be extrapolated since it was expressed when no access to the service was granted unless cookies were accepted. In this context, some regulators do not differentiate between cookie walls and paywalls, despite paywalls offering an alternative for access to the service between consent and payment;
- a principle-based approach, focusing on the ideals of free access to information and user-centric consent models; and
- a general adversity against advertising and profiling activities.

However, this stance overlooks the nuanced complexities and potential benefits that paywalls offer in balancing privacy concerns with sustainable business models.

EU regulators' emphasis on e-Privacy consent (for advertising cookies) over the broader GDPR framework (for all advertising activities) somewhat contradicts the growing adoption of paywalls. While e-Privacy regulations primarily address issues of consent and tracking in digital advertising,

they do not explicitly prohibit or discourage paywall models. However, the lack of specific guidance on paywalls in this context creates an atmosphere of uncertainty resulting from political or societal opinions instead of legal analysis resulting from the full spectrum of applicable law.

While some EU data protection authorities have issued different guidelines on conditions of lawful cookie walls/paywalls, and some have kept their silence, some other privacy regulators' apparent principle-based disapproval of paywalls conflicts with their legal acceptability, leading to a disparity between regulatory stances and the practical realities of digital content monetization.

These disparities between positions of different EU data protection regulators are likely explained by the fact that both the CJEU and the EDPB require a case-by-case approach, which does not allow for determining in each specific case what criteria may have led to the regulators' conclusion, especially when it is unfavourable to an alternative access mechanism.

Is such negative stance truly about the price of the subscription, or is it about the mere of fact subscribing to the service as an alternative? In any case, it is incumbent upon each regulator to demonstrate that the assessment criteria they have formulated are not superficial and can allow for the acceptance of some – lawful - alternative mechanisms, thereby definitively banning an unacceptable general stance according to which offering an alternative would be inherently contrary to the freedom of consent. While privacy regulators enforce data protection standards, they should ideally avoid dictating the specifics of consumer protection, civil law and competition principles applicable to digital service business models, including the use of paywalls. The current privacy-only regulatory orientation, which seems to lean against paywall models in some countries, can be critiqued for potentially overstepping this boundary. By implicitly disfavouring paywalls, regulators may be inadvertently reshaping business model choices, even where these models may comply with other regulations and are not contrary to data protection laws. This critique highlights the need for regulators to maintain an objective stance that respects the legal permissibility of various monetization strategies, including paywalls.

The current regulatory attitude towards paywalls can be criticized for potentially impeding freedom to conduct a business. By indirectly discouraging paywall models, regulators may be influencing business decisions of media and content publishers in a manner that goes beyond their mandate of ensuring data protection compliance.

This approach raises significant concerns about the freedom to conduct business, to innovate and diversify revenue streams in the digital landscape. It is crucial for all the privacy regulators to recognize a balance between protecting user data and respecting such fundamental right to determine various business models, including paywalls.

Such unified position is especially crucial in the light of the CJEU July 2023 decision that directly endorsed the possibility to offer users a fait alternatives to personalized advertising, including a paid alternative, and various EU regulations detailed below.

A comprehensive and consistent unified EU guidance adopted in the context of collaboration between data protection authorities (that would analyze the matter under privacy regulations) and competition/consumer authorities (that may intervene on pricing and marketing fairness subjects), would be necessary in order to stabilize the applicable framework ensuring the consistent regulation of business models vs. privacy considerations. A balanced approach is required, where privacy regulatory bodies acknowledge the legitimacy of paywalls under applicable laws and provide comprehensive guidelines that ensure user privacy is not compromised in paywall models.

The current regulatory stance towards paywalls, characterized, from some EU authorities, by an implicit principle-based opposition, contrasts with their legal admissibility under existing data protection frameworks. This contradiction calls for a reassessment of regulatory approaches, urging authorities to recognize the legitimacy of paywalls and to offer clear, balanced guidelines. Such guidance should accommodate the evolving landscape of digital services, ensuring that data

protection principles are harmoniously integrated with innovative business models like paywalls, thereby fostering an environment where user privacy and sustainable digital economy can coexist.

5. CONCLUSION – SUBSCRIPTION MODELS ARE REGULATED, NOT PROHIBITED

5.1 It is prohibited to prohibit alternative access mechanisms

In France, the CNIL has tried to prohibit any cookie wall as a principle: in its guidelines on cookies of 4 July 2019[22], the CNIL stated that cookie walls were unlawful not only in terms of the principle of freedom of consent, but also in terms of the doctrine of the EDPB, which considered them to be "*non-compliant with the GDPR*". However, neither the CNIL nor the EDPB at the time had defined cookie walls, nor envisaged any case-by-case analysis.

Following an appeal for annulment lodged by several professional associations and trade unions, including GESTE[23] (an association regrouping online service publishers), the French highest administrative court, Conseil d'Etat, has ruled on 19 June 2020[24] stating that the general prohibition of cookie walls contained in these CNIL's guidelines should be withdrawn as the CNIL cannot legally prohibit such practice in principle as the CNIL has not defined (i) cookie walls practice in itself, nor (ii) any factors that may allow to consider such practice compliant or not with the GDPR:

> "*the requirement of free consent cannot justify a general ban on the practice of cookie walls, as the* ***free consent of the individual must be assessed on a case-by-case basis, taking into account in particular the existence of a genuine and satisfactory alternative*** *in the event of a refusal of cookies*".

According to the conclusions of the public rapporteur before the Conseil d'Etat in the ruling of 19 June 2020, freedom of consent must indeed be assessed at an individual level:

> *"Basically, what can be discerned from the extreme diversity of situations is that* ***it is risky to assert that people who have been duly informed about the consequences of their actions would always be deprived of their freedom to consent when faced with a cookie wall, as if Internet users were all incapable adults****. It is through the complaint of a person who feels that they have been forced to consent that a debate on the possible deprivation of liberty can begin. Their own. By laying down the principle, under penalty of sanction, that the data subject, whatever his or her situation, can never freely give consent to the use of his or her personal data when the controller makes access to an Internet site or online communication service, whatever it may be, conditional on such processing, regardless of the practical consequences of refusing to consent, the CNIL therefore seems to us to have disregarded […] GDPR".*

Thus, the requirement of freedom of consent in the context of cookie walls is subject to a case-by-case analysis, governed by recitals 42 and 43 of the GDPR, according to which **the offer of an effective choice enables an individual to take a free decision, specific to a person, a context and to one or more defined purposes of processing**.

In this respect, any position that would seek to prohibit individuals from choosing, using the excuse of the consent that would be presumed not freely given, takes away from individuals their possibility to freely exercise their rights and does not reflect the spirit and objective of the GDPR.

---

22 Deliberation no. 2019-093 of 4 July 2019 adopting guidelines on the application of Article 82 of the amended Act of 6 January 1978 to read and write operations on a user's terminal (in particular "cookies and other tracers")

23 Groupement des éditeurs de services en ligne

24 Décision n° 434684 du Conseil d'Etat du 19 juin 2020, 10ème et 9ème Chambres réunies https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-19-juin-2020-lignes-directrices-de-la-cnil-relatives-aux-cookies-et-autres-traceurs-de-connexion

Drawing the consequences of this reminder from the Conseil d'Etat, the CNIL repealed and amended its July 2019 guidelines and adopted new guidelines on 17 September 2020[25], which have been in force since 1 April 2021. In this version in force, the CNIL states that cookie walls are "*likely to infringe, in certain cases, the freedom of consent*" and considers that their **lawfulness must be assessed on a case-by-case basis**, as required by the Conseil d'Etat. Some other European authorities have followed the CNIL's example and the evolutions of the market practices and accepted possible lawfulness, in principle, of cookie walls, (or at least the absence of their general prohibition), subject to some conditions:

- AEPD (Spanish Data protection authority) has updated its guidelines on cookies[26] stating that the use of cookies walls can be legal under certain conditions;
- Garante (Italian Data protection authority) considers that cookie walls may be permitted under certain conditions[27];
- Datatilsynet (Danish Data protection authority) has published guidelines containing criteria for assessing lawfulness of cookie walls[28];
- German Data Protection Conference has legitimized pay-for-use models and published evaluation criteria[29];
- ICO (UK Data protection authority) calls for a case-by-case analysis and considers genuine freedom of choice to be key in assessing lawfulness of cookie walls[30].

Other EU authorities have either kept their silence or simply repeated the EDPB's principle of prohibition of cookie walls, without analyzing their difference with paywalls nor providing any comprehensive legal assessment.

While this is not yet a position that has been accepted or considered by all of the European countries, the current regulatory trend is (and should be) user centric. Instead of a blanket prohibition of all types of cookie walls, including paywalls, a careful analysis should be made on a case-by-case basis in order to determine whether the user, who is in the centre of both target advertising based on cookies universe and data protection regulations, is aware of his or her choices and can make them in a free and informed way.

5.2 **European regulations clearly hint at paywalls possibilities**

Some might argue that while roughly a half of the EU countries have established that paywalls cannot be prohibited in principle and require a context-specific analysis, no regulation has expressly admitted or rejected lawfulness of paywalls as a general principle. Thus, should any paywall be considered unlawful until proven otherwise?

EU regulatory actively follows all of the digital trends, including the economic dependence of certain types of online services on targeted advertising (more on that below). In this context:

---

25 Deliberation no. 2020-091 of 17 September 2020 adopting guidelines on the application of Article 82 of the amended Act of 6 January 1978 to read and write operations on a user's terminal (in particular "cookies and other tracers") and repealing deliberation no. 2019-093 of 4 July 2019

26 https://www.aepd.es/documento/guia-cookies.pdf

27 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876#english

28 https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/cookies/cookie-walls

29 https://datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf

30 https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply12

- EU Consumer rights Omnibus Directive 2019/2161 expressly mentions that a service can be provided in consideration of the provision and use of personal data[31]:

  "*Given their similarities and the interchangeability of paid digital services and **digital services provided in exchange for personal data**, they should be subject to the same rules under that Directive*".

- EU Digital Content Directive 2019/770 also recognizes the provision of personal data as alternative to payment:

  "*This **Directive shall apply to any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price**.*

  *This **Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader**, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose.*"[32]

- Draft e-Privacy Regulation, in its 2021 version[33], goes even further and regulates the permissibility of cookie walls with equivalent alternative access:

  "*In contrast to **access to website content** provided against monetary payment, where access is provided without direct monetary payment and **is made dependent on the consent of the end-user to the storage and reading of cookies for additional purposes**, requiring such consent would normally not be considered as depriving the end-user of a genuine choice if* the end-user *is able to choose between services, on the basis of clear, precise and user-friendly information about the purposes of cookies and similar techniques, between **an offer that includes consenting to the use of cookies** for additional purposes on the one hand, and **an equivalent offer by the same provider that does not involve consenting to data use for additional purposes**, on the other hand.* […]."

In its opinion on the future e-Privacy Regulation[34], the EDPB reiterated its position according to which the cookie walls *stricto sensu*, *i.e.* a system of prohibiting mechanisms that offer users no alternative to accepting advertising cookies but to give up access to a service, are not compliant with the GDPR (its freedom of consent principle). In so doing, **the EDPB expressly accepts that fair alternatives** that do not require users, in a binary manner, to give their consent to cookies in order to access a service, **are not incompatible with the requirement for users to give their consent freely**:

"*Users should therefore be proposed with **fair alternatives offered by the same service providers**. Such principles should apply equally to all service providers, regardless of their sector of activity or of their current financing model*".

---

31 Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, Recital 31.

32 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, Article 3(1).

33 Mandate for negotiations with the European Parliament for Proposal for e-Privacy Regulation, 10 February 2021, Recital 20.

34 https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-032021-eprivacy-regulation_en

The EDPB is even calling for the criteria for assessing these alternatives to be specified in the future e-Privacy Regulation, which is the exact opposite of rejecting the principle of such alternatives, including paywalls.

Finally, ECJ case-law on Meta admits the possibility of paywalls' existence as well:[35]

> "*Thus, those users must be free to refuse individually, in the context of the contractual process, to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those* ***users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations.***"

The two adjectives used by the ECJ ("*appropriate*" and "*equivalent*"), attached to the need to offer an alternative, establish that the requirement of freedom of consent does not justify the discretionary right to access a service under any condition, but rather manifests as an informed choice by users among alternatives that do not deprive them of a certain freedom. Thus, the freedom of consent can be interpreted as the ability to choose among acceptable alternatives. It does not entail prohibiting the offering of choice to the user, since consent merely consists in making a choice.

As things stand, it is clear that the consensus among the European regulators responsible for interpreting the GDPR and the e-Privacy Directive and protecting personal data is not on the principle of the validity or invalidity of paywalls, but on the **need of practical arrangements and criteria for assessing paywalls, through the examination of "*fair alternatives*"**.

5.3 Various criteria for lawfulness of paywalls

European data protection authorities have expressed different views on criteria for assessing lawfulness of cookie walls / paywalls. While the majority of them give the most importance to a "*fair alternative*" criteria, some needlessly concentrate on granularity and specificities of the user consent.

On May 16, 2022, the CNIL has published its conditions for evaluating lawfulness of paywalls[36], after having had to adapt its position to comply with the July 2020 Conseil d'Etat ruling. Still, all of the companies on the French market that directly depend on targeted advertising revenues and for whom the cookie wall subject was one of survival-level importance (especially in the press, media and publishing sector), had to hold their breath for almost two years after the said Conseil d'Etat ruling before the CNIL's guidelines have seen the light. The CNIL has finally recognized that many free services on the Internet are financed by (personalized) advertising. The CNIL has thus confirmed that:

- Charging access to a service is not illegal (*sic!*);
- Offering an alternative between a reasonable payment and financing through advertising and cookies is not *per se* illegal;
- The combination between a paid alternative or an access financed by advertising and related cookies remains lawful, as long as the user's choice is informed, explicit and freely given amongst the alternatives offered to the user.

---

35 ECJ, 4 July 2023, Meta Platforms Inc and Others v Bundeskartellamt, C-252/21

36 https://www.cnil.fr/fr/cookie-walls-la-cnil-publie-des-premiers-criteres-devaluation

Therefore, the user's informed and explicit choice between fair alternatives such as (i) a reasonable payment or (ii) the use of advertising cookies, remains lawful and does not, in itself, infringe the requirement of a freely given consent applicable to advertising cookies.

The main criteria that the CNIL has highlighted in its guidelines are:

- **Fair alternative** (to cookies acceptance) for the user enabling him/her to access the service ;
- **Equivalence of the service** (included in the proposed alternative) offered by the same service provider;
- **Reasonable price** allowing users to have a true freedom of choice – but the **CNIL has stated that it is not its' role to elaborate on the pricing** that should be analysed on a case-by-case basis ; and
- **Limited purposes of the cookies** proposed for the paywall, *i.e.*, the service provider should only include those cookies (including advertising) in the paywall cookie choice that serve the purposes that justify the reasonable price proposed as an alternative to such cookies.

Thus the CNIL (i) did not pay much importance to the granularity of consent or any specific conditions of consent, and (ii) left service providers with a wide margin of discretion to decide on the price proposed as a payment alternative to cookies consent in their paywalls.

The Danish Data Protection Authority has established four criteria for assessing the lawfulness of cookie walls that are very similar to the CNIL's guidelines:

- **Reasonable alternative** to cookies consent – that could be a payment requirement, allowing the same service provider to offer users a content or a service similar to a "*large extent*" to a content/service offered to users having accepted the cookies;
- **Reasonable price** – however just as the CNIL, the **Danish authority stated that it is not its responsibility to go into more detail about the pricing** of content, services, etc.
- **Limited purposes of the cookies proposed for the paywall**, *i.e.*, the companies must be able to demonstrate that all the purposes for which the company requests consent form a necessary part of the proposed alternative; and
- **Limited cookies for the users who paid** - the companies may not process personal data for more purposes than what is necessary for the service in question to be delivered (unless a separate subsequent consent has been collected).

German Data Protection Conference has identified three evaluation criteria regarding the permissibility of paywall models, also largely following in the CNIL's steps but adding the consent granularity requirement:

- **Equivalent alternative –** a paid subscription should be an equivalent alternative to the service/content offered to the users that have consented to cookies;
- **Compliance with legal requirements of consent** (as included in the GDPR); and
- **Granularity of consent –** when consenting, users must be able to choose between the different purposes of cookies on a granular basis.

The **Spanish** DPA has considered that the use of cookie walls can be legal, under the conditions very similar to the ones already identified by the CNIL above:

- **the user is sufficiently informed**;

- an **alternative is offered** to access the service without having to accept the use of cookies; and

- **services of the two alternatives are truly equivalent** and offered by the **same service provider**.

The Spanish DPA has only mentioned the "*equivalent content or services*" condition, while the UK ICO vaguely refers to a "*genuine free choice*".

As a conclusion, a European consensus among the authorities that admit the lawfulness of pay or consent mechanisms and that have published some guidance on conditions of such lawfulness, seems to be around the vital importance of "*fair*" or "*equivalent*" alternative criteria, which includes **fair pricing** (left to the service providers' discretion), and **provision of equivalent services** under both cookies consent and paid subscription.

5.4 Alternatives proposed by publishers and use case examples

(a) Panorama of ad-based business models

Not surprisingly, running any business has a cost. A lot of criticism surrounding the paywall proposed by Meta is centred around an affirmation according to which users' privacy should not be for sale. However, what is priced in any paywall model is not the privacy, but the service to which a user can have access – for free or against payment.

A notion that digital services should be provided for free is ludicrous in itself. No business can be obliged to provide its services for free. The users may be allowed to access online services on an equal basis (*e.g.* net neutrality principle), but there is no legal obligation for any online service provider, regardless of its size, to provide services for free.

Even essential services, such as water, oil, gas or electricity, are provided against payment – and unlike digital services they are vital for individuals' survival. However, these businesses are based on resources that should be bought and resold and therefore cannot be provided against any other value than money.

Some price reductions in exchange for users' data have existed in our everyday lives for decades: think of all loyalty programs and loyalty awards. The majority of non-digital business such as supermarkets, retail, hotels, transportation, etc., offer various discounts to clients who accept to join their loyalty programs, to provide their birthdates or answer questionnaires. What do these companies get in exchange of the money value lost in the discounts? Data value: they can continue contacting their loyalty members, offering them more services, most often based on their preferences, and thus increase their revenue and compensate any money lost in the transaction offered for a reduced price.

Digital-based press, media and content publishers get anywhere from 90% to 100% of their revenue from targeted advertising. Such services include online publishers, service engines, online maps, online encyclopaedia, social media, etc. While not strictly based on the sale and resale of material resources, such businesses still have an important number of "non-digital" costs that they have to assume:

- Price of the online contents;

- Employees' pay;

- Various licenses and software rights;

- Data hosting;

- Functionalities of their services, their infrastructures and innovation costs;

- "Hard" physical costs, including electricity, water, etc.;
- Legal, accounting and marketing costs;
- Various service providers' costs.

Without targeted advertising, such digital businesses would be left to die and their service disappear: (i) if only a minority of users accept advertising cookies, and (ii) there is no financial alternative as in paywalls, there can be no miracle funding that can support such businesses running.

No press, media and content publisher can function financially based on contextualized or non-personalized advertisement alone, since **revenues from non-targeted advertising are 70% lower than revenues from targeted (cookie-based) advertising**. Independent data on the effectiveness of contextual advertising digital ads is scarce, therefore, its financial viability is at best uncertain. Existing studies are based on small-scale surveys and are generally led by vendors of contextual advertising solutions and intermediaries[37].

(b) **Paywalls: who pays for those who don't?**

As mentioned above, the pricing of paid subscriptions proposed within paywalls has been, for now, left by regulators at the companies' discretion – as it should be.

Various factors can be taken into account for such price determination, including:

- The costs that represents the loss of data of users that refuse personalized advertising;
- Importance of the service for the users, counted for example as an approximate that the users would be willing to receive to never use the service in question;
- Infrastructure and hosting costs;
- The share that personalized and non-personalized advertising represent for the company, etc.

No user can access an economic service for free. Online service providers are not providers of essential services, and even such essential services (water, electricity, etc.) are not provided for free as mentioned above.

Online service providers cannot be expected to assume all financial costs resulting from the users that refuse personalized advertising, especially where such personalized advertising amounts to almost the entirety of revenues of such online service provider.

Authors: *Etienne Drouard (Partner, Hogan Lovells – etienne.drouard@hoganlovells.com), Olga Kurochkina (Senior Associate, Hogan Lovells - olga.kurochkina@hoganlovells.com), and Rémy Schlich (Associate, Hogan Lovells - remy.schlich@hoganlovells.com)*

37 EU Commission, "Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers", 2023