IP, ICT & DATA PROTECTION
European Service Line

ANDERSEN

The Price of Privacy: Navigating Pay-or-Consent Models in the EU Digital Economy

> At its heart, the pay-or-consent model treats privacy as something that can be bought or traded. Instead of assuming consent by default, businesses are effectively putting a price tag on opting out of data processing.

At a Glance

The rise of pay-or-consent models reflects a broader shift in the digital economy, where access to online services is increasingly conditioned on the user either accepting extensive personal data processing or paying a fee to avoid it. While this framework is often presented as a form of user choice, it has sparked significant debate across Europe as to whether such a "choice" is genuinely free, particularly when refusing consent comes with a financial penalty.

This discussion is closely linked to the principles of the GDPR, especially the requirement that consent must be freely given, informed, and not coerced. In this context, pay-or-consent schemes raise concerns about the fairness of conditioning access on acceptance of data-driven advertising practices, and about the risk of turning privacy into a premium feature available only to those who can afford it.

In addition to data protection considerations, the document highlights how these models may also be scrutinised through consumer protection, competition law, and the Digital Markets Act, particularly where large platforms are involved. As regulators continue to assess the legality and boundaries of such practices, pay-or-consent models are becoming a key example of how the EU is reshaping the relationship between personal data, monetisation strategies, and fundamental rights in the digital environment.

1. Turning Privacy into Value: The Rise of Pay-or-Consent in the Digital Economy

In the digital economy, personal data has quietly become one of the most valuable assets a business can hold. Platforms, publishers, and app developers increasingly depend on user data to support targeted advertising, personalization, and performance analytics. What is often presented as *"free"* access to digital services is rarely free in practice, as users typically *"pay"* with their personal data, creating hidden economic value as well as legal and compliance exposure for businesses.

As data protection rules, especially in the European Union, have grown stricter, many companies have begun experimenting with a model that sits at the crossroads of compliance and commercial reality: the ***pay-or-consent*** model. Under this model, users are offered a clear choice, as they can either agree to the processing of their personal data, typically for advertising purposes, or pay a subscription fee to access the service without having their personal data processed. In this way, the model explicitly monetizes user choice, **transforming the traditional data-for-access exchange into a decision between ads and subscriptions.**

At its heart, the pay-or-consent model treats privacy as something that can be bought or traded. Instead of assuming consent by default, businesses are effectively putting a **price tag on opting out of data processing**. Proponents see this as a step toward honesty in the digital marketplace. This framing is not merely theoretical: academics, Data Protection Authorities, Competition Authorities, national courts, and the Court of Justice of the European Union have all acknowledged that users often *"pay"* for digital services with their personal data rather than money. The value exchange is no longer hidden, as users can clearly see what they are giving up and what they are getting in return, and they are invited to choose what matters more to them, data or money.

A key question is whether this choice is truly free. Many online services are no longer optional luxuries, but instead they are essential tools for information, communication, and participation in modern everyday life. When access depends on agreeing to extensive tracking or excessive data harvesting, payment may feel less like an alternative and more like a surcharge for protecting one's rights. **This tension is not only a matter of user perception but also a growing regulatory concern, with potential consequences for compliance, trust, and competitive positioning.**

Notwithstanding the attractiveness of this model for smaller businesses, **the broader implications cannot be ignored.** If privacy becomes something only paying users can afford, the risk of a two-tier digital ecosystem grows. Those with greater means may opt out of tracking, while others are left with little real choice aside from accepting it. This controversy challenges long-standing principles of privacy as a fundamental right, rather than as a premium feature.

As ***pay-or-consent*** models continue to spread across the EU, they raise important questions for businesses about trust, fairness, and long-term viability. Understanding how these models fit within EU data protection law is not just a legal necessity, but a strategic one, shaping how companies balance growth, compliance, and user relationships in an increasingly privacy-conscious market.

2. The EU Rules Businesses Can't Ignore

While ***pay-or-consent*** models may appear commercially attractive, they sit under intense regulatory scrutiny in the European Union. The controversy is not about innovation itself, but about whether asking users to *"pay or okay"* **genuinely respects freedom of choice.** From a regulatory perspective, payment can easily become a form of pressure, one that undermines the validity of consent and exposes businesses to legal risk.

At the heart of the debate is a simple question: is consent still freely given when refusal comes at a cost? EU data protection authorities, such as the Austrian authority on the "pay or ok" model adopted by an Austrian newspaper website, have repeatedly stressed that consent loses its meaning if users are effectively penalized for saying no. When access to a service is conditioned on payment, especially at a level most users are unlikely or unable to afford, regulators may view the model as coercive rather than voluntary. This concern is particularly relevant where the data processing in question is not strictly necessary for delivering the service itself.

For certain large platforms the regulatory bar is even higher. Under the Digital Markets Act (DMA), designated **"gatekeepers"** face specific obligations aimed at preventing coercive data practices. In some circumstances, gatekeepers must offer users an equivalent version of their service without being forced to consent to extensive

data processing. The DMA does not ban monetization, but it leaves much less flexibility for companies with strong market power and highly dependent users. Businesses that fall within the DMA's scope must therefore assess not only pricing, but whether their alternatives are genuinely comparable in quality and functionality.

Consumer protection law adds another layer of risk. *Pay-or-consent* model interfaces must be designed with extreme care. If pricing structures, data uses, or consequences of each option are unclear, authorities may classify them as misleading practices. Likewise, aggressive design tactics, such as framing payment as an unreasonable burden or nudging users through visual or psychological pressure, can trigger enforcement under EU consumer law. **Transparency is not just best practice; it is a legal requirement.**

Competition law further complicates the picture, particularly for dominant players. When platforms with significant market power use pay-or-consent models to force users into privacy trade-offs, this may amount to an exploitative abuse under Article 102 of the Treaty on the Functioning of the European Union (TFEU). Excessive subscription fees or unfair trading conditions linked to data surrender can attract scrutiny, especially where users have no realistic alternatives. In this context, privacy is no longer just a compliance issue, but it becomes a competition concern.

For businesses, the takeaway is clear: pay-or-consent models cannot be treated as a one-size-fits-all solution. Companies must assess their market position, user dependency, pricing strategy, and interface design to determine whether their model creates unfair conditions. What may be defensible for a small business in a competitive market could be unlawful for a dominant platform. In the EU, the rules centre around the principle that monetization must not come at the expense of genuine choice. Businesses that understand and respect this balance will be better positioned to innovate sustainably without turning regulatory risk into a hidden cost of doing business.

3. Key Business Risks of Pay-or-Consent Models under EU Privacy and Competition Law

The ***pay-or-consent*** model presents significant strategic challenges for businesses considering similar approaches. While it may appear to reconcile monetisation with privacy obligations, the risks for organisations are substantial and multifaceted.

Businesses implementing pay-or-consent models risk breaching the **GDPR.** As consent obtained under economic pressure is unlikely to be deemed "freely given", making data processing unlawful **exposes organisations to fines of up to 4% of global annual turnover** and corrective orders that can disrupt operations. Beyond financial penalties, enforcement actions often involve mandatory redesign of consent flows, creating costly compliance projects.

For businesses classified as gatekeepers under the **DMA**, the stakes are even higher. Failure to comply can result in **fines of up to 10% of worldwide revenue and daily penalties for ongoing breaches.** Even companies outside the gatekeeper designation face indirect risk, as regulators may extend similar fairness principles to other dominant platforms, creating uncertainty and compliance burdens. Moreover, adopting a model that restricts user choice or monetises privacy can t**rigger competition law** scrutiny.

Investigations can lead to behavioural remedies, structural changes, and reputational harm, all of which carry significant operational and financial implications.

The perception that privacy is a paid privilege also **undermines trust and brand integrity.** Businesses risk being portrayed as commoditising fundamental rights, which can alienate privacy-conscious consumers and advocacy groups. Negative press coverage and social media backlash amplify these effects, creating long-term reputational damage that outlasts regulatory penalties.

Data ethics and compliance have also become critical factors in **investor due diligence.** A monetisation model perceived as discriminatory or exploitative can erode investor confidence and strain relationships with strategic partners. This reputational risk translates into tangible business consequences, including reduced access to capital and diminished partnership opportunities.

Consumers are increasingly prioritising privacy when choosing digital services. A pay-or-consent model may accelerate user migration to competitors offering privacy-friendly solutions without financial barriers. This erosion of market share can undermine advertising revenue and subscription growth, forcing businesses into costly pivots. Although for Meta this may not seem to be the case, given there are no obvious social media alternatives with such network effects. For businesses operating in other

technology industries, they may not hold the same dominant and unique positions as Meta, resulting in a possibility of losing customers to other competitor solutions.

Besides that, consumer organisations and regulators actively promote privacy-centric alternatives, influencing user behaviour and shaping market expectations. Therefore, businesses that fail to adapt, run the risk of falling behind and losing their competitive advantage, as the market leans towards the more ethical use of data. Consumer groups and advocacy organisations, such as the European Consumer Organisation (BEUC) and NOYB are also increasingly litigious in challenging pay-or-consent models. Defending claims under data protection and consumer law adds legal costs and management distraction for businesses, while adverse judgments can set damaging precedents. Legal challenges frequently necessitate prompt revisions to consent mechanisms, subscription pricing models, and user interface designs. Implementing these modifications typically entails substantial allocation of legal, technical, and operational resources for businesses. For organisations with international operations, achieving compliance across multiple jurisdictions further increases both complexity and associated costs.

4. Turning Privacy Challenges into Opportunities: Business Tips for the EU Digital Economy

As regulatory scrutiny intensifies, businesses must move beyond compliance checklists and embed privacy principles into their commercial strategies. The following recommendations provide actionable steps to mitigate risk and create sustainable, user-centric models.

Design Alternatives: Contextual Ads and Minimal Data Processing

Businesses should explore monetisation strategies that do not rely on extensive personal data collection. Instead of behavioural profiling, **using contextual ads** based on page content or searches benefits both users as well as providing an alternative business model. In this way, reliance on sensitive data is reduced while maintaining advertising revenue streams for business that rely significant on advertising.

From a data processing perspective, offering subscription tiers or free versions that

process only essential data for service delivery is perhaps a more privacy-oriented option. Limiting data collection to what is strictly necessary demonstrates compliance with the GDPR's data minimisation principle and reduces businesses from exposure to enforcement actions.

Clear User Choice Without Coercion

Transparency is critical to building trust and meeting legal standards. This can be achieved through simple but effective methods such as:

- **Using Plain Language Interfaces:** Presenting choices in clear, concise language, whilst avoiding technical jargon, enables users to understand what they consent to.
- **Presenting Genuine Alternatives:** Business must ensure that that opting out of personalised ads does not involve punitive pricing or degraded functionality. Coercive designs such as dark patterns invite regulatory scrutiny and reputational harm for businesses and are to be avoided.
- **Implementing Layered Information:** Using layered notices that provide essential details upfront to users, with links to more comprehensive explanations is a structured and transparent way terms can be presented to users.

Compliance integrated Into Product Design

Compliance should not be an afterthought; it must be integrated into product and service developments. Businesses must embed data protection principles such as purpose limitation and data minimisation, into system architecture and service delivery from the outset.

Additionally, before implementing such a monetisation model involving personal data, a Data Protection Impact Assessment (DPIA) must be conducted. This assessment enables a business to identify risks early and provide documentation for regulators, should the business model adopted by the business be challenged.

Cross-functional governance, should also be a priority. By establishing collaboration between legal, product, and engineering teams, business can ensure compliance is embedded throughout the lifecycle, reducing costly redesigns later.

Avoid Exploitative Conditions and Dominance Abuse

Businesses with significant market power must tread carefully to avoid antitrust violations. Pricing structures must be implemented fairly, by ensuring subscription fees are proportionate and not designed to coerce consent. Excessive pricing can be construed as exploitative under competition law.

Any options offered to users in monetisation models should be meaningful and should not restrict user autonomy. Dominance abuse claims often arise when users have no viable alternative to invasive data processing.

In a pro-active approach, businesses can also consider monitoring practices against evolving competition law standards, particularly in jurisdictions where regulators are actively challenging pay-or-consent models. This will ensure a business is up-to-date with developments in this field.

Competitive Advantage: Privacy as a Differentiator, Not a Privilege

Rather than treating privacy as a premium feature, businesses should position it as a core value proposition. There are several ways in which business can ensure privacy is given the central role it deserves:

- **Implement Privacy-Centric Branding** by communicating commitments to user rights as part of business brand identity. This builds trust and attracts privacy-conscious consumers.
- **Adopt Innovative Monetisation Models**, through exploration of revenue streams that align with ethical data practices, such as free models or partnerships that do not compromise user autonomy.
- **Adopt Market Leadership Through Ethics**, to enable the business to establish itself as privacy leader. This enables businesses to gain a competitive edge, particularly as regulators and consumers converge on higher standards of data protection.

Embedding these recommendations into business strategy is not merely about avoiding fines; it is about future-proofing operations. By designing alternatives,

ANDERSEN

ensuring transparency, integrating compliance into product development, respecting competition law, and leveraging privacy as a differentiator, businesses can mitigate legal and reputational risks while strengthening their market position.

5. Final Thoughts

The evolution of monetisation models, particularly pay-or-consent frameworks, demands heightened scrutiny from businesses and regulators alike. Ensuring that users are provided with meaningful, non-restrictive choices is essential to prevent dominance abuse claims and to uphold user autonomy.

By actively monitoring the shifting landscape of competition law and responding to regulatory challenges to pay-or-consent models, businesses can adapt and remain compliant. Furthermore, embedding privacy as a central element, rather than considering it a privilege, enables companies to navigate these complex challenges. Ultimately, prioritising privacy within monetisation strategies is not only a safeguard against legal and reputational risks, but also a catalyst for long-term trust and growth in a market increasingly shaped by consumer rights and regulatory oversight.

Contact information:

Themistoklis Giannakopoulos |
European IP, IT, Data Protection Service Line Coordinator
Andersen Legal in Greece
themistoklis.giannakopoulos@gr.AndersenLegal.com

Danielle Mercieca | Senior Associate
Chetcuti Cauchi advocates Member firm of Andersen Global
danielle.mercieca@ccmalta.com

Alexandra Athitaki | Associate
Andersen Legal in Greece
alexandra.athitaki@gr.AndersenLegal.com