LUISS

Department of Law

Course of Data Protection

CONSENT AT THE CROSSROADS: BALANCING DATA PROTECTION AND MARKET REGULATION

Prof. Filiberto E. Brozzetti
SUPERVISOR

Prof. Antonio Punzi
CO-SUPERVISOR

Leonardo Lazzaro - 166833
CANDIDATE

Academic Year 2024/25

"Like Janus, personal data has two faces: one is the protection of private life, the other is its value as an economic asset".

Alain Rallet, 2018

Abstract

This dissertation arises from the awareness that we are currently witnessing a fundamental revaluation of consent, not merely as a formal checkbox, but as a substantive, dynamic expression of individual autonomy. Recent technological developments, growing regulatory complexity, and pivotal case law have pushed the boundaries of how consent is defined, interpreted, and applied in the digital age.

Chapter 1 lays the theoretical groundwork by tracing the evolution of consent in data protection law. It begins by outlining the post-GDPR paradigm shift, moving from implicit to unequivocal consent, and explores how consent operates as an expression of a fundamental right. Special attention is paid to the role of institutional actors such as the WP29 and the EDPB in shaping the operational definition of consent. This chapter also investigates the interplay between consent and new regulatory instruments like the Data Governance Act (DGA) and the Digital Services Act (DSA), highlighting the growing tension between user autonomy and systemic *consent fatigue*.

Chapter 2 moves from theory to application, analyzing how courts and regulators have interpreted consent in practice. It focuses on the shift from the illusion of "free" services to the widespread adoption of "consent or pay" models. The chapter discusses the increasing overlap between data protection and competition law, examining key cases such as *C-252/21*, *C-21/23*, and recent developments in Italy involving the AGCM and the Garante. It concludes with a reflection on the need for cooperative frameworks between authorities.

Chapter 3 expands the analysis by exploring the diverse approaches adopted by European Data Protection Authorities towards the "consent or pay" model. Through a comparative overview of decisions and guidelines from key national regulators, the chapter highlights both convergences and divergences in enforcement. It then examines the European Commission's April 2025 decision finding Meta in breach of the Digital Markets Act, framing it within the broader regulatory debate. The chapter concludes by evaluating alternative solutions beyond binary consent models, advocating for a balanced, coherent approach that reconciles data protection rights with market efficiency.

To cite this Dissertation:

MLA Lazzaro, Leonardo. "Consent at the Crossroads: Balancing Data Protection and Market Regulation". 2025.

APA Lazzaro, L. (2025). Consent at the crossroads: Balancing data protection and market regulation.

ISO 690 LAZZARO, Leonardo. Consent at the Crossroads: Balancing Data Protection and Market Regulation. 2025.

Table of contents

Introduction 10

CHAPTER 1.

A closer look at consent in data protection law

1.1 The concept of consent in data protection law 11

1.1.1 The post-GDPR paradigm shift: from implicit to unequivocal consent 13

1.2 Defining consent 18

1.3 Consent as an expression of a fundamental right 22

1.4 The freedom to consent 24

1.5 The role of WP29 and the EDPB in shaping the definition of consent 26

1.5.1 Pre-GDPR interpretations by WP29 27

1.5.2 The EDPB's Guidelines and evolving perspectives 28

1.6 Consent within the framework of the DGA and DSA regulations 31

1.7 The challenges and limitations of consent 33

1.8 The *consent fatigue* and the vulnerable data subject 37

CHAPTER 2.

Recent developments on consent and market regulation in European jurisprudence

2.1 The evolution of consent in case law: interpretations, applications and emerging trends 40

2.2 From the illusion of free online platforms to the rise of "consent or pay" models 50

2.3 The ongoing debate: antitrust and privacy in the digital economy 52

2.4 The implications of Case C-252/21 60

2.4.1 Meta Platforms Ireland v. EDPB: Meta's appeal against Opinion 08/2024 and its dismissal by the General Court 76

2.4.2 BEUC's latest evaluation of Meta's Pay-or-Consent Policy for 80

online users
2.5 Case C-21/23 83
2.6 *Actio finium regundorum* between the Italian Competition Authority (AGCM) and the Italian Data Protection Authority on unfair commercial practices: the Council of State's ruling on the appeal against Judgment No. 15326 of 18 November 2022 86
2.7 Integrating market and competition factors into data protection practices: the EDPB's position paper (January 2025) 94

CHAPTER 3.

Latest developments and future directions

3.1 The approach of European Data Protection Authorities to the "consent or pay" model 97
3.1.1 The ICO's approach 98
3.1.2 The Norwegian Data Protection Authority's approach 100
3.1.3 The Dutch Data Protection Authority's approach 101
3.1.4 The Belgian Data Protection Authority's approach 101
3.1.5 The Spanish Data Protection Authority's approach 102
3.1.6 The Austrian Data Protection Authority's approach 102
3.1.7 The French Data Protection Authority's approach 103
3.1.8 The German Data Protection Authority of Lower Saxony's approach 104
3.1.9 The Italian Data Protection Authority's approach 104
3.2 Meta found in breach of the Digital Markets Act: European Commission's April 2025 Decision 108
3.3 An alternative third option beyond the "consent or pay" model 112
3.4 Balancing data protection and market efficiency: towards a coherent regulatory approach 114
3.5 Conclusions 116

Bibliography 119
Legislation, acts and documents 127
Relevant decisions 131
List of abbreviations 132

Introduction

In the age of algorithmic personalization, behavioral profiling, and pervasive data flows, the concept of consent stands at a critical crossroads. What once appeared as a clear expression of individual will – an informed, voluntary act of autonomy – now risks becoming a checkbox exercise, often stripped of substance and shaped by opaque power structures. This dissertation explores the evolution of consent in the context of data protection, analyzing its doctrinal foundations and its trajectory in recent jurisprudence. It aims to make readers more aware of the shifting dynamics between user autonomy and market-driven data practices, especially as regulatory authorities grapple with practices such as *pay or okay* models and the commodification of consent.

At the heart of this inquiry lies a fundamental tension: can consent remain a genuine safeguard of personal freedom when it is increasingly framed as a transactional good rather than a legal right? Drawing from both legal theory and regulatory developments, this work examines how recent cases illustrate the pressing need for deeper cooperation between data protection authorities and competition regulators. Privacy cannot be treated as a self-contained world. Rather, it is a vital region of a broader empire, within which dialogue and cross-disciplinary approaches are essential.

"The truth is that meaningful consent takes time, while the acceleration of time does not allow for it. What we must ask, then, is how to reconcile the speed of online browsing with a form of consent that does not betray what we would truly want - if fully informed - regarding the use of our data. The question, perhaps, concerns not only time, but also our cognitive processes and their entanglement with modes of communication."[1] It becomes worth asking whether this dialogic dimension of consent might be recoverable precisely through interaction with artificial intelligence—technologies that are already capable of speaking and, perhaps soon, of asking users how they wish their data to be handled, illustrating possible implications, and faithfully executing those preferences in real time.

As highlighted, among others, by Kessler, Rakoff, and Slawson, issues of power imbalance, limited choice, and formalism have long affected the validity of consent. This dissertation shows how the digital ecosystem exacerbates these concerns and argues that tools fostering understanding and trust may help restore consent as a meaningful, dialogical process.

[1] Punzi, A. (2024). In Cerrina Feroni, G., Commerciabilità dei dati personali. Profili economici, giuridici, etici della monetizzazione. Il Mulino.

CHAPTER 1.

A closer look at consent in data protection law

Summary: **1.1** The concept of consent in data protection law - **1.1.1** The post-GDPR paradigm shift: from implicit to unequivocal consent - **1.2** Defining consent - **1.3** Consent as an expression of a fundamental right - **1.4** The freedom to consent - **1.5** The role of WP29 and the EDPB in shaping the definition of consent - **1.5.1** Pre-GDPR interpretations by WP29 - **1.5.2** The EDPB's Guidelines and evolving perspectives - **1.6** Consent within the framework of the DGA and DSA regulations - **1.7** The challenges and limitations of consent - **1.8** The *consent fatigue* and the vulnerable data subject

1.1 The concept of consent in data protection law

The notion of consent in European data protection law has its roots in long-standing philosophical debates, closely linked to the principles of human dignity and autonomy. Manson & O'Neill argue that the discussion on informed consent originates from the Age of Enlightenment and the birth of the social contract theory, which was based on the fundamental idea that freely expressed consent could legitimise otherwise impermissible actions.[2] In particular, autonomy is commonly recognised as the conceptual pillar at the basis of consent.[3] In the Kantian perspective, autonomy is the individual's right to self-determination and to act in accordance with his or her own conception of good. Consent is therefore the embodiment of the philosophical trend that builds legal relationships on the basis of individual will.[4]

Starting from the 19th century, with the affirmation of the principle of self-determination, concepts such as individual sovereignty and freedom of choice have acquired a prominent role in the legal landscape.[5] However, it is only with the Charter of Fundamental Rights of

[2] Manson, N. C., & O'Neill, O. (2007). Rethinking informed consent in bioethics. Cambridge University Press.

[3] Kosta, E. (2013). Consent in European data protection law. Martinus Nijhoff Publishers.

[4] This voluntarist philosophy is inherited in particular from the work of Immanuel Kant, who saw in individual will the expression of a universal legislation, which he called moral law and whose source lies in the autonomy of the will. Kant, E. (1788). Critique of Practical Reason.

[5] Feinberg, J. (1982). Autonomy, sovereignty, and privacy: Moral ideals in the constitution. Notre Dame L. Rev.

the European Union[6] and with the Treaty of Lisbon[7] that the right to the protection of personal data has obtained autonomous recognition: these Treaties laid the foundations for a legal system where consent to data processing is enshrined as a fundamental expression of individual self-determination, elevated within the framework of jus cogens.

Consent plays an important role in legitimising data processing: the function of consent is precisely to perpetuate the 'bond of trust' between the various actors.[8] Specifically, in the field of personal data protection, consent has the dual function of establishing the legitimacy of personal data processing and allowing the data subject to exercise control over their personal data.

Whilst it was clear from the outset that the institutional concept of consent was based on robust ethical principles, it was not as clear how this should be translated into practice. The extremely rapid evolution of technology and the proliferation of new applications made it necessary to introduce regulations aimed at defining clear criteria for valid consent.

However, regulating a constantly changing environment has proven to be an arduous and never-ending task: each new regulation was soon superseded by the development of innovative technological tools, quickly rendering the legal provisions adopted obsolete or ambiguous.

As will be illustrated below, the evolution of consent in European data protection law can be divided into two main distinct approaches, each introduced (or intended to be introduced) to correct the shortcomings of the previous one. We can identify presumed consent, introduced with the Data Protection Directive[9], and explicit consent, consolidated with the General Data Protection Regulation[10] (hereinafter referred to as the 'GDPR').

---

[6] European Union. (2000). Charter of Fundamental Rights of the European Union. Official Journal of the European Communities, 2000/C 364/01.

[7] European Union. (2007). Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community. Official Journal of the European Union, 2007/C 306/01.

[8] Stoeklé, HC. (2017). Toward dynamic informed consent. Med Sci (Paris).

[9] European Union. (2016). 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, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119/1.

[10] European Union. (1995). 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. Official Journal of the European Communities, L 281/31.

1.1.1 The post-GDPR paradigm shift: from implicit to unequivocal consent

The adoption of the GDPR has increased the complexity of the existing regulatory framework at both the European and national levels, in order to respond to technological developments and new models of economic growth[11] with technologically neutral protection rules, which apply regardless of the technique used and whether or not the data processing is automated.[12] While the system of definitions and fundamental concepts relating to the identification and roles of the subjects involved, and their rights and duties, is retained, albeit with some modifications, the GDPR modifies the basic structure of the rules on the processing of personal data, as per Directive 95/46/EC (also referred to as the *parent directive*) and domestic legislation, with regard to organisational and business models and the obligations of data controllers and processors.[13] With administrative obligations reduced (despite the re-emergence of obligations to compile documents recording processing activities), processing, under the conditions of the law, is carried out 'at the risk' of the data controller and other subjects involved from time to time.[14] The Regulation also identifies a series of measures to be adopted by the data controller, which tend to be preventive in nature, but these are requirements that focus on the organisational structure of a company and on technological tools as a means of protection. By way of example, we can think of Data Protection Impact Assessment or Privacy Impact Assessment[15], in case of high risk to rights, freedoms, and individuals; the design of systems and applications aimed at minimising the use of personal data[16] (so-called *privacy by design* and *by default* - art. 25), technical and

[11] As stated by Recital 6 of the GDPR, technological advancements and globalization have intensified data protection challenges, increasing data collection and processing. The Recital emphasizes the need for individuals to retain control over their personal information.

[12] As stated by Recital 15 of the GDPR, data protection principles apply universally, regardless of the processing technique used or whether the processing is automated.

[13] Giannone Codiglione, G. (2016). Risk-based approach e trattamento dei dati personali.

[14] As stated by Recital 89 of the GDPR, the reduction of administrative burdens for data controllers is explicitly addressed.

[15] For further details, reference is made to Recital 84 ff. and Article 35 ff. of the GDPR, which outline the importance of assessing and mitigating risks associated with data processing, including the requirement for DPIAs.

[16] For further details, reference is made to "Privacy by Design" Principles explained by Dr. Ann Cavoukian.

organisational measures aimed at minimising the risk to personal data (such as pseudonymisation); the mandatory appointment, in selected cases, of a new control figure, the Data Protection Officer. These measures are aimed at making the data controller (art. 24 and art. 2) accountable[17] for the adoption of procedures capable of avoiding risks to the data, under penalty of heavy administrative fines (up to 4% of the previous year's annual worldwide turnover); or – but here, however, without significant changes compared to the previous regulatory framework – compensation (art. 82).

The adoption of the Data Protection Directive represented a decisive step in responding to the growing concerns about privacy deriving from technological progress and the increasing number of processing activities. Recital 4 of the Directive emphasised how the use of personal data was increasingly widespread in various economic and social sectors, while also highlighting that the evolution of information technologies had made the collection and exchange of such data easier.

According to Article 2(h) of Directive 95/46/EC, consent was defined as a freely given, specific and informed indication of the data subject's wishes by which the individual signifies agreement to the processing of personal data relating to them. Article 7(a) clarified that consent should be unambiguous, while Article 8(a) imposed an additional requirement of explicitness for the processing of special categories of data. In addition, the Directive recognised the right of data subjects to be informed about how their data would be used and to object to the processing in certain circumstances.

However, after the directive came into force, a significant issue emerged: although the legislator had tried to ensure that consent was indeed voluntary, the wording of Article 8 suggested that explicit consent was not always necessary to make data processing lawful. This led to the proliferation of passive consent models, in which the user's simple inaction, such as not refusing, was interpreted as tacit acceptance.[18] Consequently, even though consent constituted only one of the legal bases for lawful processing, it quickly became the mechanism most used by data controllers to demonstrate privacy compliance. This favoured the spread of permissive privacy policies, often based on opt-out models, in which the user was automatically included in the data processing unless they decided to revoke their consent. This led to a practical problem: the burden of exercising their rights fell on data subjects,

[17] Art. 5, GDPR.

[18] Carolan, E. (2016). The continuing problems with online consent under the EU's emerging data protection principles. Computer Law & Security Review.

who often found themselves having to deal with complex procedures to protect their privacy, especially in a context of increasing technological sophistication and increasingly technical legal language.

Another critical issue that emerged was the assumption that users were capable of making truly informed decisions. Although the directive aimed to guarantee an informed choice, it did not adequately consider whether the data subjects had the necessary skills to assess the risks associated with the processing of their data. In many cases, not giving consent meant not being able to access certain services, making the choice not truly uncoerced.[19] Over time, it became clear that most users had a limited understanding of the digital environment and its implications, making it impractical for them to effectively exercise their rights under the legislation then-applicable.

To address issues such as these, the ePrivacy Directive[20] was adopted in 2002 with the aim of integrating Directive 95/46/EC and updating the regulatory framework to take account of the new challenges set by the digital world.[21] This directive aimed to strengthen the protection of personal data with respect to emerging tools such as spyware, web bugs, hidden identifiers and cookies, imposing the obligation to provide clear and accessible information to users before obtaining their consent. The need to address these risks was emphasised in recitals 5 and 6.

However, the new regulation was based on the assumption that users were able to fully understand the information provided and act accordingly. Considering that Directive 95/46/EC had already highlighted the limits of an approach based on user proactivity, it was foreseeable that simply providing more information would not increase the level of awareness. As highlighted by Carolan[22], the same behavioural tendencies that inspired the directive undermined its effectiveness: with the increasing complexity of online services, even the most attentive users struggled to understand the real impact of the utilisation of their data, while privacy policies remained extensive, highly technical and not easily accessible.

---

[19] Ibid.

[20] European Union. (2002). Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. Official Journal of the European Communities, L 201/37.

[21] European Parliament and Council. (2002, July 12). 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.

[22] Ibid.

In 2009, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (hereinafter referred to as the Article 29 Working Party) highlighted further critical issues, emphasising that the growing complexity of data collection practices, business models and technologies often exceeded the ability or willingness of users to make truly informed decisions about sharing their information.[23]

Another problematic issue introduced by the ePrivacy Directive concerned the regulation of direct marketing and advertising based on cookies. Recital 40 stated that explicit consent was required for any unsolicited commercial communication, but did not provide the same strict standard for other types of processing. Furthermore, Recital 25 legitimised the use of cookies and tracking technologies, provided that users were clearly informed and had the opportunity to object. This allowed continued use of opt-out models, especially in behavioural advertising, where a lack of refusal was interpreted as tacit acceptance.

The directive also paved the way for 'take-it-or-leave-it consent' models, where access to services could be made conditional on the acceptance of cookies. This led to the adoption of coercive mechanisms, where the user had no real alternative other than to accept the processing in order to use the requested service. Over time, numerous European institutions recognised that the ePrivacy Directive had neglected fundamental aspects, including the presence of forced consent mechanisms, unnecessary data processing and conditionality in access to services (Article 29 Working Party[24]; European Commission[25]; European Data Protection Supervisor[26]).

Finally, the lack of legal clarity has led to conflicting interpretations in the various Member States, with regulations ranging from the obligation of written consent to implicit acceptance. This regulatory inconsistency has made the urgency of clearer regulatory intervention evident, leading to the development of the GDPR.

---

[23] Article 29 Data Protection Working Party. (2009, 1 December). The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data.

[24] Ibid.

[25] EC. (2010, November 11). Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions.

[26] EDPS. (2015, July 27). Opinion 3/2015 (with addendum). Europe's big opportunity EDPS recommendations on the EU's options for data protection reform.

Given the framework described above, it is clear that for many years consent was the cornerstone of data protection law. The underlying idea was to give precedence to the individual's will and decision-making autonomy. The Data Protection Directive framed consent as the pre-eminent legal basis, with additional ones being considered only as residual. This concept was also transposed when the directive was implemented by the Italian legislator. In this sense, reference should be made to art. 23 Legislative Decree 30.6.2003, n. 1962, now repealed, which followed the aforementioned approach.[27] Consent to the processing of personal data for specific purposes was therefore seen as a way of safeguarding informational self-determination, the highest expression of a will that is informed, specific and, above all, free, not coerced or even influenced. The rationale behind this approach was based on a society in which the diffusion of internet means was not yet widespread, and it was believed that the expression of will conferred by users to individual processing operations could take place in a conscious manner and in line with the normative dictates. With the spread of social networks and numerous online applications, the expressions of will to be released by individual users have increased exponentially and, consequently, the legislator has had to question the mechanism of consent as a pre-eminent condition of lawfulness. In fact, with the approval of the GDPR in 2016, there has been a paradigm shift: as far as so-called common data is concerned, i.e. data that does not belong to particular categories, consent now represents only one of the possible and alternative legal bases.[28] This approach is part of the broader principle of accountability: the data controller has the responsibility, in order to respect the principle of lawfulness as understood therein, to determine the most appropriate legal basis for their actions, choosing the most suitable one from among those provided. This legislation did not set out a prohibition but rather established an evaluation parameter to be considered together with other relevant factors that come into play in each specific case. The aim was precisely to avoid reducing the expression of will to a mere fictitious clause of legitimacy of the negotiating and technological power of others.[29] Therefore, as a parameter of validity with respect to an activity that involves a right of personality, consent today operates on a new, additional level that is not

[27] Italy. (2003). Legislative Decree No. 196/2003 of June 30, 2003, on the Protection of Personal Data (Privacy Code), as amended by Legislative Decree No. 101/2018. Official Journal of the Italian Republic, No. 174.

[28] Borgobello, M. (2023). Manuale di diritto della protezione dei dati personali, dei servizi e dei mercati digitali. Milano.

[29] Alpa, G., & Resta, G. (2019). Le persone e la famiglia. Vol. 1: Le persone fisiche e i diritti della personalità. Torino.

superimposable with respect to the manifestation of the negotiating will of a user who intends to use a specific service. Moving on to the post-GDPR framework, in articles 7 and 8, this regulation imposes certain requirements for consent to be considered validly given: the person must be adequately informed about the processing that will be carried out; have an effective, specific and free choice; be able to refuse or withdraw consent without suffering prejudice. In the case of consent given by a minor, there are additional conditions of validity, given the intrinsic fragility of the minor compared to an adult.

These requirements lead to the assumption that the legislator wanted to embrace a concept of consent intended more as authorisation than as a contractual nature: a consent that expresses not so much the will, but the personality of the data subject and that, therefore, as such, cannot have a patrimonial nature.[30]

For the purposes of validity, particular focus is then placed on the need to monitor any situation of weakness of the individual, which will be discussed below, in particular both from the point of view of the evident 'asymmetry of information' and the unbalanced position between the latter and the data controller, and from the point of view of ensuring protection against possible aggressive commercial techniques.[31]

1.2 Defining consent

The preliminary analysis highlights that the data subject's informative self-determination serves as the primary mechanism for balancing, on one hand, the need to protect the individual to whom the data pertains, and on the other, the interests of the data controller. According to the provisions of art. 6 and art. 9 GDPR, consent constitutes the first and most important condition for the legitimacy of the processing. Given its central role as a balancing tool between often conflicting needs[32], it is useful to focus on its legal definition, characteristics, and classification[33], as well as the related critical issues.

Article 4, paragraph 1, no. 11) of the Regulation refers to consent as a voluntary, specific, informed, and clear expression of will, through which the individual explicitly agrees, either

[30] Thobani, S. (2016). I requisiti del consenso al trattamento dei dati personali. Roma.

[31] Manganello, G. (2020). Consent and the illusion of autonomy in EU data protection: the necessary utopia.

[32] Namely, those of the data subject and the data controller.

[33] Bravo, F. (2017). Il consenso e le altre condizioni di liceità del trattamento dei dati personali. Bologna, Zanichelli.

by a statement or a definitive affirmative action, to the processing of their personal data[34], by means of a statement or by a clear affirmative action.[35] It is therefore an act of acceptance of the data processing[36], the form of which must be expressed[37] and the manifestation of which must be unambiguous[38]. In accordance with Recital 32 of the GDPR, silence, lack of action or pre-ticked boxes cannot be considered valid forms of consent.[39]

With reference to the fundamental characteristics of consent, freedom cannot be considered as respected if the refusal to give it compromises the real possibility of choice of the data subject or if there is a risk of deception or coercion.[40] The requirement of specificity is only satisfied if the consent concerns a clearly defined processing, thus excluding generic forms of consent without a defined purpose.[41] The consent must also be informed, which implies that the concerned party receives all essential information about the processing in a clear and understandable way. In this sense, the GDPR distinguishes between cases in which the data is collected directly from the concerned party and those in which it is obtained from third parties, regulating the relative information in articles 13 and 14 of the Regulation.

The privacy policy is an essential condition to guarantee the individual's self-determination and must indicate precisely, already at the moment of data collection, the specific purposes of the processing.[42] If the privacy policy is incorrect, it can compromise the validity of the

---

[34] In assessing whether consent is freely given, particular attention should be paid to whether the performance of a contract, including the provision of a service, is made conditional on consent to the processing of personal data not necessary for the performance of that contract, as outlined in Article 7(4) of the GDPR.

[35] In the literature, it is observed that the notion of consent outlined by the Regulation is more comprehensive than that of Directive 95/46/EC. Basunti, C. (2020). La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali.

[36] This is clearly evident from the reading of the first two sentences of Recital 32 of the GDPR.

[37] Bravo, F. (2017). Il consenso e le altre condizioni di liceità del trattamento dei dati personali. Bologna, Zanichelli.

[38] By way of example, Recital 32 of the GDPR refers to forms of consent such as written declarations, including those provided electronically, or oral statements.

[39] Recital 32 of the Regulation also provides that "Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them".

[40] Pizzetti, F. (2016). Privacy e il diritto europeo alla protezione dei dati personali. Giappichelli.

[41] Resta, G. & Zeno-Zencovich, V. (2018). Will and Consent in the Provision of Services on the Internet.

[42] In this regard, the guidance set out in Recital 39 of the Regulation.

consent subsequently expressed by the data subject.[43] Finally, consent must be unequivocal, meaning that it must not give rise to ambiguity or doubts about the data subject's willingness to accept the processing. Giving consent generates a legal relationship between the parties, which can have a fixed or indefinite duration, and the proof of consent is up to the data controller, as stated in art. 7, par. 1, of the GDPR.[44]

One of the most significant novelties introduced by the Regulation is the explicit recognition of the right to withdraw consent at any time.[45] Such revocation has immediate effect and does not affect the lawfulness of the processing carried out on the basis of the previously given consent. To ensure the effective exercise of this right, the data subject must be informed of the possibility of revocation from the moment the data is collected and must be able to exercise it with the same level of ease as when giving consent.[46] Furthermore, the revocation can take place without the need to provide reasons, unlike the objection to the processing regulated by art. 21 GDPR.

As for the legal qualification of consent, there are different doctrinal interpretations. According to an initial approach, already developed with law no. 675/1996 and legislative decree no. 196/2003, consent does not give the data subject power of disposition over their personal data, since the latter are not comparable to an object of property, but rather fall under the category of fundamental human rights. From this perspective, consent does not involve the transfer of personal data, but represents an authorisation that legitimises its processing, which would otherwise be illegal.[47]

A different theoretical approach recognises the economic dimension of personal data, considering them as goods that can be exchanged. From this point of view, the consent of the individual takes on the nature of a dispositive act, allowing the circulation of data on the market. This orientation, while admitting the personalistic nature of the data, considers it possible to configure dispositive acts similar to those recognised for other personality rights,

---

[43] Colapietro, C. & Iannuzzi, A. (2017). I principi generali del trattamento dei dati personali e i diritti dell'interessato. Napoli, Editoriale Scientifica.

[44] Bravo, F. (2017). Il consenso e le altre condizioni di liceità del trattamento dei dati personali. Bologna, Zanichelli.

[45] This seems to have resolved the doctrinal debate on the temporal boundaries of the exercise of the right to withdraw.

[46] Thus, Article 7, paragraph 3, of the Regulation.

[47] Rodotà, S. (1995). Tecnologie e diritti. Bologna, Il Mulino.

such as the right to one's image.[48] According to this view, the data subject can therefore consent to the processing of his or her data, without this implying a waiver of the right to their protection.

Other interpretative positions consider consent as an advance waiver of protection, an element of a complex legal case or a pact not to exercise the right. However, the legislator has provided a detailed regulation of the rights of the individual concerned, mitigating the implications deriving from the different legal qualifications of consent.

The above analysis highlights the importance of consent among the conditions of lawfulness of the processing: it allows the data subject to participate in the process of circulation of his or her personal data, legitimising the processing and, to a certain extent, influencing the methods of their transfer.[49] Through consent, therefore, the task of balancing the protection of one's data with the need to share it is entrusted to the data subject. Furthermore, the importance of consent is reinforced by its recognition in the Charter of Nice, whose Article 8 establishes that the processing of personal data must take place on the basis of the consent of the data subject or of another legal basis foreseen by the law.

Although consent continues to play a central role, the prevailing doctrine has observed that it has lost the prominent function it had under Directive 95/46/EC.[50] In the current European regulatory context, in fact, the principle of private autonomy as the basis for the lawfulness of processing has been scaled back. This legislative choice is motivated by the fact that, often, the freedom of consent remains only formal and not substantial, translating into an adherence that does not guarantee adequate protection of the interested subject. Since the rules for data processing are generally established unilaterally by the data controller, consent often amounts to mere passive acceptance.[51] The information asymmetry between data controllers and data subjects, together with the complexity of privacy policies, leads users to accept the conditions without fully understanding them.

---

[48] In this regard, see Cass. Civ., Section 1, judgment of January 29, 2016, no. 1748.

[49] Mazzamuto, S. Il principio del consenso e il problema della revoca.

[50] Caggia, F. (2019). Libertà ed espressione del consenso. Torino, Giappichelli.

[51] Ibid.

1.3 Consent as an expression of a fundamental right

As briefly outlined in the preceding sections, analysing the framework of consent in the current context certainly implies reflecting on the functions of self-determination of the data subject, with particular attention to consent as the exercise of a fundamental right of the individual. This is because consent to the processing of personal data is considered an integral part of the fundamental right to the protection of personal data, as established by Article 8 of the Charter of Fundamental Rights of the European Union. Article 8 not only configures consent as an action that can represent a *legitimate basis* for the processing of personal data[52] but also uses consent to place the protection of personal data among the 'freedoms' outlined in Title II of the same Charter.[53]

While art. 7 of Directive EC/95/46 defined consent as a prerequisite for the legitimacy of the processing, separating, at least apparently, the concept of legitimacy from that of lawfulness pursuant to art. 6 of the same Directive, the GDPR directly associates the lawfulness of the processing with the definition of its legal basis, assigning to art. 6 the task of balancing individual, collective and public interests, typical of the regulation of fundamental rights. In this context, the consent of the data subject stands out as the legal basis that combines the protection of personal data and the self-determination of the individual, leaving the latter with the task of balancing interests, while for the other legal bases this balancing is delegated to the legislator, the supervisory authority and the judge.[54]

As observed by legal doctrine, this does not exclude that the evaluation of the lawfulness of consent may require further balancing, in particular when the processing to which consent is given is functional to an illegal activity that damages the interests of the subject or third

[52] Orlando, S. (2022). Per un sindacato di liceità del consenso privacy. Persona e Mercato.

[53] See the Opinion of AG M. Szpunar, 4 March 2020, *C-61/19, Orange v. Romania*, para. 36: "The requirement of consent of a data subject is a central feature underlying EU data protection law. It features in the Charter of Fundamental Rights of the European Union, where it is stipulated in Article 8 that data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by the law. Seen in a wider context, the concept of consent allows the data subject concerned to decide for him or herself on the legitimacy of restrictions to on his or her right to the protection of personal data".

[54] This holds true only partially in cases where the processing of personal data is necessary for the performance of a contract. Although, in such instances, necessity must be assessed purely objectively, regardless of any awareness or involvement of the data subject, their participation in the determination of data processing and the assessment of the relevant interests at stake cannot be entirely excluded (see Court of Justice of the European Union, 4 July 2023, Meta Platforms, C-252/21).

parties.[55] The constitutional dimension of consent as an expression of the fundamental right to self-determination is clearly illustrated by the Opinion of Advocate General Szpunar in *Orange v. Romania,* who emphasized that consent serves as a means for individuals to autonomously determine the legitimacy of any restrictions on their right to data protection. Moreover, the core principle of EU data protection law is rooted in the concept of individual self-determination, recognizing each individual as the holder of his or her own personal data. In this perspective, the Court of Justice tends to interpret legal bases other than consent restrictively, considering them as exceptions to the rule, anchored to the consensual legal basis, as an expression of a fundamental right.[56]

Furthermore, in this context, a restrictive interpretation of the rules on non-consensual bases of processing is linked to the principle of legitimate expectations. According to a distinctive vision of the European approach, the constitutional matrix of consent as an instrument for exercising freedom of self-determination has guided its discipline, both with regard to the criteria for assessing the integrity of the will and in relation to the link between consent and contract.[57] The free, informed, manifest and specific nature of consent to treatment does not allow its validity requirements to be equated with those of any act of private autonomy. Unlike the latter, consent must respect the principle of effective protection of fundamental rights, which, although tempered by the principle of proportionality, tends to favour the data subject, even to the detriment of the trust of the data controller or processor.

Consequently, it is not enough for consent to follow the logic of adhesion contracts: for the Court of Justice, it is necessary that consent be "effectively read and assimilated"[58], much more than simply known or knowable. The Court has recently reiterated the importance of consent being given "with full knowledge of the facts", in particular regarding the purposes of the processing and the dissemination of the processed data.[59]

---

[55] Ibid.

[56] See Court of Justice of the European Union, 4 July 2023, Meta Platforms, C-252/21.

[57] Comparative law often highlights the differing approaches on either side of the Atlantic, emphasizing the constitutional foundations of personality rights. In Europe, these rights are primarily rooted in the concept of human dignity, whereas the North American perspective tends to focus on the paradigm of liberty, particularly as freedom from state interference. On the more recent developments in U.S. law, see Hartzog, W. & Richards N. (2020). Privacy's Constitutional Moment and the Limits of Data Protection. Boston College Law Review.

[58] See Court of Justice of the European Union, 11 November 2020, Orange v. Romania, Case C-252/21.

[59] See Court of Justice of the European Union, 4 July 2023, Meta Platforms, C-252/21.

The unequivocal manifestation of consent excludes it from being implicit or passive, requiring instead an active and manifest declaration by the data subject.[60] From this derives the specificity of consent, which cannot be inferred from acts of autonomy that are simply connected to it, as in the case of a request for a service. As with all legal bases, consent is linked to specific purposes of the processing, and therefore its specificity is an essential condition.[61]

1.4 The freedom to consent

Consent and freedom are also expressed today in two areas that appear to be increasingly close: that of contracts and that of the processing of personal data. If, in fact, until some time ago the distinction between property and non-property was clear, now it is no longer so evident. It is widely known that for a long time the debate on consent (and therefore on the freedom of consent) in contracts and that on consent (and therefore on the freedom of consent) in the processing of personal data have proceeded along two different and parallel tracks, which were assumed to be destined never to meet: on the one hand that of contracts and property rights, and on the other that of personal rights and non-property and inalienable rights. Now the two tracks no longer seem inevitably parallel but intertwine in ways that are not entirely obvious. The discussion on freedom takes place in both identified areas: on the one hand, the area of contractual freedom of negotiation and, on the other, the area of freedom in the protection of personal data. Freedom concerns the phase of formation of the will and the phase of expression of the will: therefore, it is freedom *of,* and *in the* expression of consent. Once the necessary information has been acquired, the will is free in its formation and then, in the absence of coercion, including technological coercion, in its expression. From a normative point of view, therefore, it is necessary to consider the provisions regarding contracts in general, those regarding contracts with consumers and then those concerning the processing of personal data. [62]

[60] See, with reference to Article 4(11) GDPR, Court of Justice of the European Union, 19 October 2019, Planet49, Case C-673/17; Orange v. Romania, Case C-252/21, cited above.

[61] Ibid.

[62] Finocchiaro, G. (2024). Consenso al trattamento e libertà. Libertà e liceità del consenso nel trattamento dei dati personali. Firenze, Persona e Mercato.

When discussing the requirements for consent, both in the context of negotiation and in the context of personal data protection, the requirement of freedom already has a central position in the normative framework, which becomes even more important in light of the recent jurisprudential and doctrinal orientations that will be explained below.

On closer analysis, both in the context of negotiation and that of the processing of personal data, freedom is not absolute, but rather subject to limits.

In the contractual context, freedom has not coincided exclusively with the manifestation of the will of the contracting parties for some time now.[63] As Irti emphasised, today we find ourselves in an era characterised by exchanges without agreements and no longer dominated by the principle of autonomy of the will.[64]

The process of forming one's will, as well as the evaluation of the degree of contractual freedom, can no longer be limited to the subjective dimension of the parties. Instead, it is necessary to consider parameters external to the contracting party that affect the genuineness of the manifestation of will.

It is then fundamental that this determination has not been influenced by phenomena of abuse, which enrich and complicate contractual discipline. The vices of consent are not limited to those provided for by the civil code, which entail the annulment of the contract, but also include cases which, although not formally falling under the vices of consent, alter the contractual balance and may give rise to remedies for damages.[65]

Consequently, freedom of contract is defined in relation to elements external to the individual sphere. The phrase "within the limits imposed by law" now takes on a broader meaning, acquiring new nuances in light of abusive practices identified by both European and national legislators. In this context, contractual freedom extends beyond the merely individual dimension.

Sacco, in some of his writings on contracts, observed that for a party to be able to express a conscious will, they must be free, have the ability and time to reflect, as well as possess the necessary knowledge and information.[66]

---

[63] A significant example in this regard is the decision of the Italian Supreme Court, First Civil Section, 25 May 2021, No. 14381, which focused on the requirements for valid consent in the context of automated processing of personal data aimed at generating reputational profiles.

[64] Irti, N. (1998). Scambi senza accordo. Rivista trimestrale di diritto e procedura civile.

[65] Gentili, A. & Cintio, V. (2018). I nuovi "vizi del consenso". Contratto e impresa.

[66] Sacco, R. (2016). Il contratto. Milano.

However, in a context of immediate exchange, such as the digital one, where the decision is made in the instant of a click, these conditions cannot always be met.

Freedom, therefore, is not to be sought solely in the material act of clicking, but in the context and the assumptions that determine the conditions. This contextual vision is also supported by the most recent European regulations on digital issues, such as the *Digital Services Act* (DSA)[67], which imposes specific information obligations on platforms, the structuring of transparent decision-making processes and the introduction of corrective measures such as blackouts or sanctions.

A different concept of will and freedom is thus taking shape, one that emerges even before the contractual sphere with regard to the protection of personal data. The two areas, once considered distinct, now intersect and influence each other, giving rise to new interpretations that were previously difficult to imagine.

1.5 The role of WP29 and the EDPB in shaping the definition of consent

From the outlined framework we have observed that the definition and practical application of consent have been subject to continuous refinement, particularly in response to the challenges posed by digitalization, big data, and artificial intelligence. The interpretation of consent has been significantly shaped also by two key European bodies: the Article 29 Working Party (WP29) and its successor, the European Data Protection Board (EDPB). These institutions have provided authoritative guidance on the conditions under which consent can be considered valid, informed, and freely given, influencing both legislative developments and enforcement practices across the European Union.

Before the General Data Protection Regulation came into force, WP29 played a central role in developing the conceptual framework for consent under Directive 95/46/EC. Through various opinions and working documents, WP29 established foundational criteria that emphasized the necessity of genuine autonomy in the consent-giving process. Notably, Opinion 15/2011 on the definition of consent highlighted the importance of avoiding coercion and ensuring that individuals retain meaningful control over their personal data.

[67] 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 (Digital Services Act).

These early interpretations laid the groundwork for the more stringent consent requirements introduced under the GDPR.

With the adoption of the GDPR in 2018, the EDPB inherited WP29's legacy and expanded upon its work, refining the definition of consent in light of new technological and regulatory challenges. The EDPB's Guidelines on Consent under Regulation 2016/679 (Guidelines 05/2020) provided further clarity on the conditions of valid consent, particularly concerning issues such as conditionality, withdrawal, and the role of dark patterns in undermining user autonomy. The Board has also addressed the evolving landscape of digital services, where the increasing reliance on behavioral advertising and AI-driven profiling raises critical concerns about the genuine freedom of user choices.

This section will first examine WP29's pre-GDPR interpretations of consent, exploring how its early opinions influenced the regulatory framework that culminated in the GDPR. It will then analyze the EDPB's approach, focusing on its evolving perspectives in response to contemporary challenges, including algorithmic decision-making, personalized advertising, and the complexities of consent in online environments. By tracing this evolution, it becomes evident that the definition of consent is not static but continuously shaped by legal, technological, and societal developments.

1.5.1 Pre-GDPR interpretations by WP29

In 2011, at the request of the European Commission, the Article 29 Working Party issued an Opinion[68] aimed at clarifying the requirements for valid consent under the applicable legal framework. This document underscores that an individual's autonomy is both a prerequisite for and a consequence of consent. However, this principle is subject to limitations, and the effectiveness of consent as a mechanism for self-determination is closely tied to its application in appropriate contexts and the presence of the elements mandated by law. Notably, consent cannot be exploited by data controllers as a means of shifting responsibility onto individuals: its validity does not exempt the controller from fulfilling their legal obligations. In a more thorough examination, the WP29 played a crucial role in shaping the pre-GDPR interpretation of consent under Directive 95/46/EC and the e-Privacy Directive.

[68] WP29. (2011). Opinion 15/2011 on the definition of consent.

In Opinion 15/2011, WP29 analyzed the legal framework of consent, emphasizing that it must be freely given, specific, informed, and unambiguous. It clarified that consent is only valid if based on a clear, affirmative action and distinguished it from the right to object under Article 14 of Directive 95/46/EC. The Opinion criticized practices where consent was bundled, coerced, or vaguely implied warning that such approaches rendered data subject control illusory. WP29 also advocated for a demonstrability obligation, requiring data controllers to provide evidence that valid consent had been obtained.

Building on this, Opinion 04/2012[69] addressed cookie consent under the amended e-Privacy Directive (2009/136/EC), reinforcing the principle that storing or accessing information on users' devices requires prior informed consent. However, it introduced exemptions for cookies used solely for communication transmission (e.g., load balancing cookies) or those strictly necessary for a service explicitly requested by the user (e.g., shopping cart cookies). WP29 rejected broad interpretations of these exemptions, ruling out their application to analytics, behavioral advertising, or third-party tracking technologies.

By Opinion 02/2013[70], WP29 further clarified valid consent mechanisms for cookies, directly addressing misleading industry practices. It ruled that mere continued browsing was insufficient to infer valid consent, as users must perform an active, affirmative action, such as clicking an "I accept" button. It also stressed the importance of granular consent, requiring websites to allow users to choose different levels of cookie acceptance rather than forcing an all-or-nothing approach. The Opinion aligned with earlier WP29 positions on transparency and accountability, insisting that consent must be revocable and obtained before data processing begins.

These pre-GDPR interpretations directly influenced Article 4 (11) GDPR, which formalized WP29's concerns into law by requiring consent to be a clear, informed, affirmative action, thereby rejecting pre-ticked boxes, implied consent, and coercive practices. The WP29's work thus laid the foundation for the modern EU data protection framework, strengthening data subject control and ensuring more rigorous consent standards.

[69] WP29. (2012). Opinion 04/2012 on the meaning of consent.

[70] WP29. (2013). Opinion 02/2013 on apps on smart devices.

1.5.2 The EDPB's Guidelines and evolving perspectives

The evolution of the interpretation of consent by the EDPB reflects a progressive tightening of the requirements to ensure genuine user control over personal data.

Initially, in 2018[71], the focus was on international data transfers under Article 49 GDPR, where consent was considered a derogation rather than a standard mechanism for legitimizing data flows. The EDPB emphasized that explicit consent in this context had to be clearly informed, specific to the transfer, and unambiguous. The guidelines introduced the principle that consent must be given with full awareness of the risks associated with data transfers to third countries lacking an adequacy decision or appropriate safeguards. Importantly, the EDPB reinforced that relying on consent as a basis for transfer should be exceptional, as opposed to a routine practice, and data exporters were urged to first seek appropriate safeguards before resorting to consent-based transfers.

Subsequently, in 2020[72], the EDPB further refined its interpretation of consent under the GDPR, expanding on the requirements of Article 4(11). The guidelines clarified that for consent to be freely given, there must be a real choice, meaning that individuals should not be coerced or placed in a position where refusal would result in detrimental consequences. The issue of power imbalance was a key concern, particularly in situations where an individual's ability to refuse consent was effectively compromised, such as in employment relationships or interactions with dominant online platforms. The EDPB explicitly prohibited practices like bundling consent with other terms of service, ensuring that individuals could access services without being forced to consent to unnecessary data processing.

Another major development was the insistence on granularity, meaning that consent should be given separately for different purposes rather than as a blanket approval. This was particularly relevant for digital services, where companies often sought broad undefined consent covering multiple processing activities. Additionally, the EDPB ruled that mere continued browsing, scrolling, or inactivity could not constitute valid consent, as users must engage in an affirmative action that unmistakably indicates their intention to consent.

[71] EDPB. (2018). Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.

[72] EDPB. (2020). Guidelines 05/2020 on consent under Regulation 2016/679.

This clarification was crucial in addressing deceptive design patterns that nudged users into unknowingly agreeing to data collection.

Furthermore, by 2024[73], the EDPB turned its attention to the growing phenomenon of "consent or pay" models, which have been increasingly implemented by large online platforms. These models typically present users with a binary choice: either consent to the processing of personal data for behavioral advertising or pay a fee to access the service without tracking. The EDPB found that, in most cases, such models fail to meet the criteria for freely given consent. One of the key concerns was the issue of detriment: if refusing consent means paying a significant fee or losing access to an essential service, then the choice is not genuinely free. The guidelines emphasized that consent should not be used as a means to pressure users into accepting invasive data processing, particularly in contexts where the platform holds a dominant market position or where network effects make alternative services difficult to access.

Furthermore, the EDPB raised concerns about conditionality, stating that controllers must provide an equivalent alternative that does not involve payment if they wish to rely on consent as a lawful basis. This stance aligns with the *Bundeskartellamt* ruling from the CJEU, which will be further explored later, which held that users refusing consent must be offered an alternative version of the service that does not rely on behavioral advertising. The EDPB also stressed that companies should explore less intrusive business models, such as contextual advertising that does not require extensive personal data collection.

This evolution in the interpretation of consent demonstrates a clear trend toward stricter and more protective standards. The EDPB's approach has shifted from ensuring that consent is properly informed and explicit to tackling more complex issues related to coercion, economic pressure, and market dynamics. Over time, the Board has moved to close loopholes that could allow controllers to undermine user autonomy by designing consent mechanisms that are formally compliant but practically ineffective.

The overarching principle guiding this evolution is that data protection is a fundamental right, not a commodity that individuals should have to pay to preserve. The EDPB has also reinforced that controllers must not exploit consent as a mere procedural requirement but must ensure that it functions as a genuine expression of user intent. The emphasis on revocability, meaningful alternatives, and the prohibition of coercion reflects a more

[73] EDPB. (2024). Opinion 08/2024 on valid consent in the context of consent or pay models implemented by large online platforms.

robust interpretation of the GDPR's core principles, ensuring that individuals retain true control over their personal data in an increasingly digital and data-driven world.

1.6 Consent within the framework of the DGA and DSA regulations

Finally, in the ongoing debate on the role of consent as a legal basis for the processing of personal data, a central role is played by the analysis of the numerous recently introduced regulations that have contractually formalised or recognised the contractualisation[74] of a series of relationships based on the voluntary provision and processing of personal data.
These include the Digital Content Directive ('DCD')[75], the Omnibus Directive[76], the Data Governance Act ('DGA'), the DSA[77] and the Data Act[78].
New perspectives on the concept of consent are therefore emerging, and with them new challenges to be faced.

---

[74] The debate on the contractualization of relationships involving the processing of personal data is highly heated. For a reasoned and up-to-date analysis of the different positions, along with relevant bibliographic references, see, for all, Ricciuto, V., Consenso al trattamento e contratto.

[75] Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services. Particularly relevant is the following provision of Article 3(1) DCD: "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".

[76] Directive (EU) 2019/2161**,** amending Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC, and 2011/83/EU for better enforcement and modernization of Union rules on consumer protection. Particularly relevant is Article 4, point 2(b) of the Omnibus Directive, which introduced Article 1a into Directive 2011/83/EU, containing a provision consistent with the aforementioned Article 3(1) DCD: "1a. This Directive shall also apply where the trader supplies or undertakes to supply digital content which is not supplied on a tangible medium 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 which is not supplied on a tangible medium 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".

[77] The relevant provisions of the DSA include those allowing recipients of online platform services to modify the parameters of the advertising targeted at them (Article 26 DSA) and the options influencing the parameters of recommendation systems that determine the order of the information presented to them (Article 27 DSA).

[78] The Data Act is particularly relevant for its provisions on contractual data sharing between businesses and consumers (B2C) and between businesses (B2B), including the sharing of data generated through the use of connected products and related services, as defined therein (Chapters II and III, Articles 3-12 Data Act). Additionally, it addresses unfair contractual terms in agreements between businesses concerning data access and use (Chapter IV, Article 13 Data Act).

One of the most current issues concerns the possibility, introduced by the DGA, of expressing one's consent to data altruism[79], i.e. the destination of personal data for purposes of collective interest. The DGA promotes this practice with the aim of incentivising the use of personal data as a common good.[80]

However, in this context, the principle of specific consent is called into question, since the user cannot know in advance or be informed in detail about the future processing of their data.[81] A similar problem arises in the case of automated data processing: users provide initial consent for processing whose boundaries are difficult to define and whose explanation is particularly complex. As early as 2018, data protection authorities from around the world, at the "International Conference of Data Protection and Privacy Commissioners – ICDPPC" entitled "Debating Ethics: Respect and Dignity in Data Driven Life", they adopted the *Declaration on Ethics and Data Protection in Artificial Intelligence*, laying the foundations for a structured reflection on the ethical and social implications of these technologies.

With the arrival of the AI Act[82], the debate has returned to the center of attention: in this context, consent plays a fundamental role in protecting the individual, safeguarding them from the risk of exploitation of personal data – understood as fragments of their identity – and from possible manipulation.

---

[79] Data altruism is defined as the voluntary sharing of data based on the consent given by data subjects for the processing of their personal data or on authorizations granted by other data holders to allow the use of their non-personal data, without requesting or receiving compensation beyond the reimbursement of costs incurred to make their data available, for objectives of general interest established in national law, where applicable. These objectives include healthcare, combating climate change, improving mobility, facilitating the processing, production, and dissemination of official statistics, enhancing the provision of public services, policymaking, or scientific research in the public interest (Article 2(16) DGA).

[80] In a joint opinion, the EDPB and the EDPS highlighted potential inconsistencies arising from the interplay between the GDPR and the proposed DGA. These include the need to reference the GDPR's definition of 'consent' and the interactions between data subjects' consent and data altruism. See Joint Opinion EDPB-EDPS 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act), 9 June 2021.

[81] Poggi, A. & Fabbrizi, F. & Savastano, F. (2023). Social network, formazione del consenso e intelligenza artificiale. Itinerario di un percorso di ricerca di Beniamino Caravita.

[82] Reg. (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, establishing harmonized rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139, (EU) 2019/2144, and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828, establishing a common regulatory framework for AI, with the aim of fostering innovation, safety, and the protection of fundamental rights in the use of AI technologies within the European Union.

The AI Act goes even further, removing even individual will (and therefore consent) from some data processing considered highly risky from a democratic point of view, such as those related to social scoring systems inspired by the Chinese social credit system model.

The use of technologies characterised by a high demand for data also brings to the fore another much-debated issue: the monetisation of data, or the 'data in exchange for services' model. The wide availability of personal data allows for detailed analyses on specific groups of users, pushing companies to collect as much information as possible. While this practice should not be demonised, as it offers concrete advantages such as the personalisation of services, it is clear that it challenges the current architecture of personal data protection, at least in appearance.

Irrespective of that, although all these sources explicitly reaffirm the pre-eminence of the GDPR, there is still no systematic theoretical framework in European legal doctrine capable of integrating these regulations into a coherent and shared conceptual vision, going beyond the simple affirmation of the supremacy of the GDPR. In the absence of a harmonised theory, this statement risks being reduced to a declaration of principle with no real practical effect and is unsuitable for providing clear guidance in the interpretation and application of the regulations, especially when dealing with the numerous practical issues that are already emerging.[83]

1.7 The challenges and limitations of consent

As said, the recognition of consent as a lawful basis for data processing reflects the broader societal emphasis on individual autonomy in decision-making. This ability to grant or withhold consent in appropriate contexts serves as a means of safeguarding personal autonomy and ensuring a degree of control over one's data.[84]

However, for consent to serve as an effective tool of autonomy, it must be both informed and voluntarily given, with the added requirement that individuals should be able to withdraw it at any time without adverse consequences.[85]

[83] Ricciuto, V. (2024). Consenso al trattamento e libertà. Consenso al trattamento e liceità. Firenze, Persona e Mercato.

[84] Richards, N., & Hartzog, W. (2019). The Pathologies of Consent. Washington University Law Review.

[85] CIPL. (2024). The limitations of consent as a legal basis for data processing in the digital society.

While consent may serve as a suitable and effective legal basis in certain well-defined contexts, its overall adequacy as the primary mechanism for legitimising data processing is increasingly undermined by the intricacies of modern data ecosystems.

The evolving nature of digital interactions and the scale of data flows expose inherent limitations in relying on consent as the foundation for lawful processing. Firstly, the expectation that individuals provide explicit consent for each specific purpose proves increasingly impractical in a digital landscape characterized by pervasive and dynamic data flows, raising concerns about its scalability. Additionally, the sheer volume and complexity of information that individuals must process to make informed decisions impose a disproportionate cognitive and informational burden, potentially undermining the very autonomy that consent aims to protect. Moreover, certain data processing activities extend beyond individual decision-making, affecting third parties in ways that individual consent alone cannot adequately safeguard.

These challenges suggest that while consent remains a valuable legal tool, its practical limitations necessitate a reconsideration of its role in data protection frameworks, particularly in contexts involving large-scale and automated data processing.

Furthermore, a key aspect of the European Commission's digital strategy[86] recognizes that data is not solely a commercial asset but also holds significant societal value, often extending beyond its original purpose of collection or generation.[87] In many cases, new and beneficial uses for previously gathered data may emerge over time, even if they were not foreseeable at the moment of initial collection - when consent would typically be required prior to processing. Recital 33 of the GDPR acknowledges this challenge in the context of scientific research, permitting individuals to provide consent in a less granular manner, provided that adequate safeguards - such as adherence to ethical standards and the implementation of technical and organizational measures in accordance with Article 89(1) GDPR - are in place.

[86] The European Commission's digital strategy, introduced under the leadership of President Ursula von der Leyen, aims to shape Europe's digital future by fostering technological innovation, ensuring data protection, and reinforcing digital sovereignty. It includes key legislative initiatives such as the Digital Services Act (DSA), the Digital Markets Act (DMA), the Data Governance Act (DGA), and the Artificial Intelligence Act (AI Act). This strategy seeks to balance economic growth and innovation with fundamental rights, security, and fair competition in the digital landscape.

[87] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), Recital 6.

A framework that allows individuals to opt in to broader categories of data use, while ensuring accountability through robust ethical and security mechanisms, could offer a balanced approach to harnessing the benefits of the digital revolution while upholding fundamental rights.

Nevertheless, both the EDPB and the EDPS have asserted that obtaining consent for purposes categorized under *general interests* - outside the specific scope of scientific research, as seen in the case of data altruism under the DGA - would not be compatible with the GDPR unless a comprehensive list of such purposes were explicitly defined.[88] However, the rapid and continuous evolution of technology complicates this approach. Data itself is highly contextual, with its utility being shaped by factors such as the recipient, the moment of use, and whether it is combined with additional datasets. As technological advancements unfold, the potential applications of data similarly expand, making it difficult to predetermine an exhaustive list of permissible uses. Imposing rigid limitations risks rendering legal frameworks obsolete, as the notion of restricting data to a single, pre-defined purpose - where an individual is fully informed and makes a one-time decision - fails to reflect the complexities of the contemporary digital environment.

The traditional model of consent, therefore, faces significant scalability challenges.

Furthermore, the right to withdraw consent at any time adds another layer of complexity. For instance, in the context of private health insurance, an individual who exercises their right to withdraw consent may inadvertently prevent the insurer from fulfilling its contractual obligations, as the processing of health data - subject to consent under Article 9 GDPR - becomes legally unfeasible. This illustrates the broader implications of consent in data governance, highlighting the need for alternative mechanisms that balance individual autonomy with the operational necessities of data-driven services.

For consent to be considered sufficiently *informed*, individuals must receive all essential information regarding processing operations and their purposes. However, this requirement has made consent forms increasingly complex[89] due to the intricate nature of modern data processing practices. Even when designed in compliance with Recital 42 GDPR, ensuring

---

[88] European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act), 9 March 2021.

[89] European Data Protection Board (EDPB), Guidelines 05/2020 on Consent under Regulation 2016/679, 4 May 2020.

they are presented in an *intelligible and easily accessible form, using clear and plain language*, these forms must comprehensively outline all processing activities, and the categories of personal data involved. As a result, they tend to become excessively lengthy, ultimately undermining their intended function.

Moreover, the overwhelming frequency with which individuals encounter consent requests throughout the day renders meaningful engagement with them nearly impossible. Instead of fostering genuine user control, this inundation often reduces consent to a mere formality - a box-ticking exercise devoid of substantive decision-making. Empirical studies have highlighted the scale of this issue, estimating that a single individual would require approximately seventy-six working days per year to thoroughly read all privacy policies they are presented with. As Richards and Hartzog aptly observe, the pervasive reliance on consent has led to its overuse, to the extent that it has become significantly weakened as a legal safeguard.[90]

Digital products and services frequently interact, leading to the exchange of user data that can affect multiple individuals. In this interconnected environment, the actions of one person on a platform can have consequences for others. While the concept of consent traditionally emphasizes individual choice, in the digital context, it often intersects with the rights of third parties, including other users and platforms.

This intersection is particularly evident in areas such as fraud prevention and cybersecurity. As noted earlier, Article 5(2) of the Digital Markets Act (DMA) could potentially make cybersecurity and fraud prevention measures contingent upon user consent. Similarly, the German *Bundeskartellamt*, as will be discussed in more detail below, has suggested that general prevention measures should also require consent. In these cases, requiring consent for data processing could extend to malicious actors, effectively demanding their approval for measures aimed at detecting fraudulent or harmful activities.[91]

[90] Neil Richards and Woodrow Hartzog, (2019). The Pathologies of Consent, Washington University Law Review, op. cit.

[91] Nettesheim, M. (2020). Data Protection in Contractual Relationships (Art. 6(1) (b) GDPR), in The EU General Data Protection Regulation (GDPR).

1.8 The *consent fatigue* and the vulnerable data subject

The so-called *consent fatigue*, combined with the growing complexity and multiplicity of requests for consent, risks compromising its original function, making it be perceived as a mere bureaucratic formality without any real meaning. *Fatigue*, in general, has been described as an unpleasant experience that emerges when an individual fails to achieve the expected objectives, leading to frustration, disillusionment and cynical attitudes.[92]

This concept can be divided into two phases: an initial over-solicitation of the user, followed by a progressive habituation.

The guidelines of the Article 29 Working Party have highlighted the negative effects that the GDPR and the multiplicity of requests for consent – particularly in the context of online browsing – can generate. It is emphasised that users, subjected to continuous requests to authorise the processing of their data, may develop a sort of automatism that leads them to no longer read the information provided before giving consent. This undermines the effectiveness of the protections provided, making consent a mere formality, rather than an instrument of informed control.[93]

This phenomenon has been widely studied by legal experts, who have shown that the people involved, overwhelmed by the number of decisions to be made, tend to opt for the simplest choice, often automatically accepting the default option.[94] This *fatigue* is caused by various factors, including the demand for decisions that exceed the user's processing capacity[95], the excessive availability of alternatives[96], and the difficulty of fully understanding the meaning and implications of consent.[97]

---

[92] Choi, H., et al. (2018). The role of privacy fatigue in online privacy behaviour. Computers in Human Behavior.

[93] Article 29 Working Party, Guidelines on Consent under Regulation (EU) 2016/679, adopted on 28 November 2017, last revised and adopted on 10 April 2018.

[94] Choi, H., et al. (2018). The role of privacy fatigue in online privacy behaviour. Computers in Human Behavior.

[95] Vohs Kathleen, D. et al. (2008). Making Choices Impairs Subsequent Self-Control: A Limited-Resource Account of Decision Making, Self-Regulation, and Active Initiative. Journal of Personality and Social Psychology.

[96] Weitzner, Daniel J. et al. (2008). Information Accountability. Communications of the ACM.

[97] This overload of information beyond the data subject's ability to comprehend it has given rise to the notion of "Information overload."

These issues have also been recognised by European legislators, as evidenced in the proposed e-Privacy Regulation, which emphasises that consent collection mechanisms should be as simple and clear as possible. In fact, it has been noted that the proliferation of tracking cookies and similar techniques has led to an exponential increase in requests for consent, submerging users in an excessive number of notifications.[98]

The language adopted by both scholars and legislators clearly reflects the emotional impact of this situation on data subjects: terms such as "fatigue", "overload" and "weariness" fall within the lexical field of negative emotions. These emotions, in turn, influence the way individuals manage their privacy, making them reluctant to actively control their data.[99]

Some scholars link the phenomenon of *consent fatigue* to the so-called *privacy paradox*, according to which individuals end up sharing their data not because they really want to, but because the authorisation process is excessively burdensome.

Once again, for consent to be legally valid, it must be freely given, informed, specific and unambiguous. However, if requested too frequently, it risks losing its effective awareness, transforming itself into a mechanical and meaningless action. In this regard, Richards and Hartzog emphasised that consent is only truly effective when the user has the time and resources to consider its consequences in a considered manner.[100]

The proliferation of requests for consent, instead of increasing the user's control, ends up undermining it, depriving it of the ability to effectively manage its personal data.[101]

Paradoxically, while one might think that the increase in requests for consent guarantees greater control to the user, in reality it causes the opposite effect, namely a sense of oppression and overload.

---

[98] See, for further discussion, European Commission, 2017/0003 (COD), recital 22, which highlights the importance of providing information and obtaining user consent through intuitive methods. Given the widespread use of tracking technologies, users frequently receive consent requests, leading to an overload of such prompts. To address this issue, the regulation emphasizes the role of technical solutions, such as transparent and user-friendly settings in browsers and applications, to facilitate consent management. Browsers, acting as intermediaries between users and websites, are particularly well-positioned to help individuals control the flow of information to and from their devices, serving as gatekeepers to protect user privacy.

[99] Tang, Jie, Akram, Umair, SHI, Wenjing. (2020). Why People Need Privacy? The Role of Privacy Fatigue in App Users' Intention to Disclose Privacy: Based on Personality Traits. Journal of Enterprise Information Management.

[100] Richards, N. & Hartzog, W. (2019). The Pathologies of Digital Consent. Washington University Law Review.

[101] World economic forum. (2013). Unlocking the Value of Personal Data: From Collection to Usage. Industry Agenda.

It has been shown that the adoption of privacy management tools depends not so much on the perception of control, but on the ease of use of these tools.[102] Furthermore, some studies show that the *fatigue* of consent has a more significant impact on user behaviour than their actual concerns about privacy.[103]

In summary, user over-exposure is so widespread in the digital ecosystem that it has also attracted the attention of European institutions. The European Commission[104], the European Parliament[105], the Council of the European Union[106] and the European Data Protection Board[107] have recognised the need to regulate this phenomenon. In particular, the Council has warned that excessive demands for consent can lead to a dangerous habituation, reducing the effectiveness of data protection safeguards.[108]

[102] Jeffrey, M., Maynes, C., Lowry, P. B., & Babb, J. (2014). Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure. Paper presented at the International Conference on Information Systems. Auckland, New Zealand.

[103] Choi, H., et al. (2018). The role of privacy fatigue in online privacy behaviour. Computers in Human Behavior.

[104] European Commission, COM/2017/010 final - 2017/03 (COD), recital 22.

[105] European Parliament, Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Privacy and Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (e-Privacy Regulation), 20 October 2017, LIBE Committee, 2017/003COD, Amendment 24.

[106] Council of the European Union, 2017/0003 (COD), recital 20a.

[107] EDPB, Statement of the European Data Protection Board on the review of the ePrivacy Directive and its impact on privacy and confidentiality in electronic communications, 25 May 2018.

[108] Council of the European Union, 2017/0003 (COD), op. cit., recital 20a.

CHAPTER 2.

Recent developments on consent and market regulation in European jurisprudence

Summary: **2.1** The evolution of consent in case law: interpretations, applications and emerging trends - **2.2** From the illusion of free online platforms to the rise of "consent or pay" models - **2.3** The ongoing debate: antitrust and privacy in the digital economy - **2.4** The implications of Case C-252/21 - **2.4.1** Meta Platforms Ireland v. EDPB: Meta's appeal against Opinion 08/2024 and its dismissal by the General Court - **2.4.2** BEUC's latest evaluation of Meta's Pay-or-Consent Policy for online users - **2.5** Case C-21/23 - **2.6** *Actio finium regundorum* between the Italian Competition Authority (AGCM) and the Italian Data Protection Authority on unfair commercial practices: the Council of State's ruling on the appeal against Judgment No. 15326 of November 2022 - **2.7** Integrating market and competition factors into data protection practices: the EDPB's position paper (January 2025)

2.1 The evolution of consent in case law: interpretations, applications and emerging trends

Having examined the concept of consent from a doctrinal perspective, this section shifts its focus to the evolution of consent within case law. In particular, it explores key decisions that have significantly shaped the interpretation and application of consent, prior to the pivotal case of Case C-252/21, which will be discussed in greater detail in the following paragraphs, up to the latest developments on the subject.

At first, it should be observed that European case law has progressively emphasised the requirement of unambiguousness, especially with regard to the "dark patterns"[109] typical of the web, inferring, for example, the invalidity of pre-set consent.[110]

At the same time, looking at the national context, it is interesting to trace the developments of the case law of the Court of Cassation (elaborating the positions of the Italian Data

[109] *Dark patterns* refer to deceptive user interface designs that manipulate users into making unintended, unwilling, or detrimental choices. These design techniques exploit cognitive biases to influence behavior, often leading to consent fatigue, unintended subscriptions, or the sharing of personal data without fully informed consent. The European Data Protection Board and other regulatory bodies have recognized dark patterns as a concern in data protection and consumer law, particularly in the context of online services and digital platforms.

[110] See, in this regard, the landmark decisions of the Court of Justice of the European Union in the so-called "Planet 49" and "Orange v. Romania" cases.

Protection Authority) which, on the other hand, has highlighted the informed and specific nature of consent, requiring, for example, its renewal in the event of a change of data controller[111] or, on the other hand, information regarding the type of logic applied to an algorithm for the reputational rating of people.[112]

Therefore, the following analysis will emphasise the attention paid, both by the Court of Justice and by national regulators, to the requirements of effective freedom and awareness of consent, demonstrating how crucial informational self-determination is for the sustainable governance of platform society (and the economy).

In the Planet49 case[113], which emerged in 2013, a German company organized a promotional lottery, offering users the chance to participate by entering their personal information, such as their names and addresses. The participation form consisted of two separate sections, each paired with a checkbox. The first section asked participants to consent to receiving direct advertising from third parties, with a corresponding empty checkbox that the user had to manually check in order to proceed with entering the lottery. The second section, however, sought consent for the company to set cookies on the participant's devices, which would enable Planet49 to track users' online behavior when they visited the websites of advertising partners.[114] This consent request included a pre-ticked checkbox, which users were not required to uncheck in order to participate in the lottery. Additionally, the request featured a hyperlink that led to a webpage providing details about the different cookies.[115]

The Federation of German Consumer Organizations challenged this consent practice, arguing that it did not meet the necessary requirements of being freely given or informed, thereby initiating legal proceedings that eventually reached the Federal Court of Justice in Germany.[116] The court referred several questions to the Court of Justice of the European Union for a preliminary ruling, specifically concerning the validity of consent when a

---

111 As occurs in the so-called Tiziana Life case.

112 As occurs in the so-called Mevaluate case.

113 Planet49 case, C-673/17, judgment of 1 October 2019, delivered by the Court of Justice of the European Union (Grand Chamber), with Judge Koen Lenaerts presiding.

114 Younas, A. & Bakhodir, T.o.M (2021). To What Extent are Consumers Harmed in the Digital Market from the Perspective of the GDPR? International Journal Of Multidisciplinary Research And Analysis.

115 Case C-673/17, paragraphs 25-30.

116 Wiedemann, K. (2020). The ECJ's Decision in "Planet49" (Case C-673/17): A Cookie Monster or Much Ado About Nothing? IIC - International Review of Intellectual Property and Competition Law.

checkbox is pre-selected. This case, decided in October 2019, was the first case directly linked to the GDPR to be addressed by the CJEU.[117]

The CJEU's ruling on the case introduced crucial clarifications regarding the principles of consent under the GDPR, focusing on the concepts of specific, informed, and unambiguous consent.[118] In terms of specific consent, the Court determined that consent must reflect a direct indication of the data subject's wishes with respect to the data processing at hand. In this case, it was underlined that the consent given by individuals who entered their details into the lottery form and submitted their entries without unchecking the pre-ticked box could not be considered specific to the collection of cookies. The consent was confined to the participation in the lottery and did not extend to the consent for cookies, as the users had not actively consented to that aspect of data processing.[119]

Regarding informed consent, the court addressed the need for transparency, particularly under the ePrivacy Directive, which governs the use of cookies. The court ruled that for consent to be informed, the information provided must allow the data subject to easily comprehend the implications of their decision: information should be sufficiently clear and detailed, enabling users to understand how cookies work and what the consequences of their consent would be.[120] Moreover, the court specified that the duration of cookie storage must be disclosed, as users need to know for how long their online activities will be monitored. Additionally, it was emphasized that users should be informed about any third parties who might have access to the data collected by the cookies, and this information should include the identities or categories of the recipients of the data.[121]

The concept of unambiguous consent was central to the case, especially regarding the use of the pre-ticked checkbox and the Court concluded that passive consent, as evidenced by a pre-selected checkbox, could not meet the GDPR's requirement for consent to be an active expression of the data subject's will. For consent to be valid, it must be unambiguous,

---

[117] Kuner, p. 10; InfoCuria, Case Law, Document List.

[118] Krommendij, J. & Zuiderveen Borgesius, F. (2022). How to read CJEU judgments: deciphering the Kirchberg oracle. Eu Law Analysis.

[119] Case C-673/17, paragraphs 58-59.

[120] Solove, D. J, & Schwartz, P. M. (2021). EU Data Protection and the GPDR. Aspen Select Series, Wolters Kluwer, New York.

[121] Ibid., paragraphs 73-75.

meaning it must involve an active action from the user. In this case, the Court expressed concern that users might not have read the information provided or may not have even noticed the pre-ticked checkbox. Therefore, this method of obtaining consent was not consistent with the GDPR's standards for valid, informed, and specific consent.[122]

The Planet49 case marked a significant moment in the interpretation of consent under the GDPR, establishing essential principles that continue to guide the application of data protection laws in the European Union. It highlighted the need for clear, transparent, and proactive consent mechanisms, particularly in the context of online data collection and cookie usage.[123]

Shifting the focus to another important case, the Romanian Data Protection Authority[124] imposed a fine on Orange Romania, a mobile telecommunications provider, for processing customers' personal data without obtaining valid consent. Orange Romania had entered into written contracts for the provision of telecommunications services, which included clauses stating that customers had been informed of and had consented to the collection and storage of their identity documents.[125]

The company claimed that its sales agents had provided customers with the necessary information regarding data processing before concluding the contracts and had obtained their oral consent during phone calls. Based on this alleged consent, sales agents pre-ticked the checkboxes concerning the collection of identity document copies before presenting the contracts to customers. Those who refused to consent were required to sign a separate form explicitly confirming their refusal.

The case[126] was referred to the Court of Justice of the European Union (CJEU) by the Regional Court of Bucharest for a preliminary ruling regarding the conditions under which consent can be considered freely given, specific, and informed under the Data Protection

---

122 Ibid., paragraphs 37.

123 Santos, C., Bielova, N., & Matte, C. (2020). Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. Technology and Regulation, Tilburg University.

124 Romanian Data Protection Authority (ANSPDCP - Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal).

125 Sava, R. (2020). Unwrapping the consent box. The CJEU Judgment in the Orange Romania Case.

126 Case C-611/18, Orange Romania SA v Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM), judgment of 12 November 2019, delivered by the Court of Justice of the European Union.

Directive (DPD). However, to provide guidance on the interpretation of EU law, the CJEU ruled on the case based on both the Data Protection Directive and the General Data Protection Regulation. In its November 2020 judgment, the CJEU emphasized that consent requests must be presented in a manner that is clearly distinguishable from other contractual matters within a written declaration. However, the Court left it to the referring court to determine whether the consent checkbox was sufficiently distinct from other contractual clauses. Furthermore, the CJEU underlined that for consent to be considered freely given, the data subject must have a genuine choice, including a real opportunity to refuse or withdraw consent.[127]

Without such an option, individuals might mistakenly believe that the contract could not be concluded without providing consent. The right to withdraw consent also includes the obligation to provide information on how this right can be exercised.[128]

The Court held that consent is invalid if "the freedom to choose to object to that collection and storage is unduly affected by that controller in requiring that the data subject, in order to refuse consent, must complete an additional form setting out that refusal". However, it remained for the referring court to determine whether requiring data subjects to sign a separate refusal form constituted a restriction on their freedom of choice.[129]

Although the referring court asked the CJEU to clarify the meaning of *freely given*, *specific*, and *informed* consent, the Court did not directly address the requirements of specificity and informed consent. Instead, it commented on the ambiguity of such consent.

The Court briefly mentioned the need for unambiguous consent, referring to its previous Planet49 ruling, which established that consent must be a clear affirmative action. However, it did not elaborate on the criteria for determining whether the information provided to customers was sufficient or specific enough, and it merely held that for consent to be valid, the data controller must be able to demonstrate that it was freely given, specific, and informed.

The CJEU also concluded that a signed contract containing a clause stating that the data subject had been informed of and had consented to data processing does not constitute valid consent if the corresponding checkbox was pre-ticked or if the contract could mislead the

[127] Sava, R. (2020). Unwrapping the consent box. The CJEU Judgment in the Orange Romania Case.

[128] Case C-611/18, paragraphs 39 and 47.

[129] Ibid., paragraphs 41 and 52.

data subject regarding their right to freely given consent - particularly the right to receive information about, refuse, and withdraw consent.

In his Opinion, the Advocate General argued that if it is unclear whether the data subject has actually read and understood the provided information - as is the case with pre-ticked boxes - consent cannot be considered unambiguous. The data subject might have given consent out of pure negligence.[130]

Additionally, when assessing the case, the AG noted that while the issue was not directly raised in the referral, Orange Romania had clearly failed to demonstrate valid consent.

He argued that the lack of clarity regarding consent suggests that it was ambiguous. While he did not explicitly state that consent was inherently invalid due to ambiguity, the legal framework and case analysis implied that the consent provided in this case was ambiguous rather than merely uninformed or unspecific.

Therefore, to sum up, in the Planet49 case the German court sought guidance from the CJEU on the validity of consent in relation to pre-ticked boxes, and the latter provided clarity on the requirements for specific, informed, and unambiguous consent but did not analyze the element of "freely given" consent. It is reasonable to assume that if the validity of the first checkbox - required for participation in the lottery - had been subject to the preliminary ruling, the Court would have addressed the concept of freely given consent in greater depth. The Planet49 judgment suggests that these criteria should be treated as distinct elements, each assessed separately in different legal contexts.

By contrast, in Orange Romania, the CJEU did not provide explicit guidance on what constitutes unambiguous consent, despite identifying problematic elements that it had previously associated with ambiguity in consent. Nevertheless, the CJEU chose to highlight the essence of unambiguous consent by linking it to the lack of specificity and information in the consent process. In his Opinion, the Advocate General attempted to clarify that pre-ticked checkboxes and the difficulty of demonstrating consent inherently prevent consent from being unambiguous. However, in its final judgment, the CJEU did not explicitly attribute this reasoning to the requirement of unambiguous consent or provide a clear distinction between the different consent criteria.[131] By failing to clearly differentiate the criteria and provide specific guidance on all of them, there is a risk that the legal standards

[130] Opinion of AG Szpunar, Case C-61/19, Orange România SA v ANSPDCP, paragraph 45.

[131] Sava, R. (2020). Unwrapping the consent box. The CJEU Judgment in the Orange Romania Case.

for consent become ambiguous themselves, making interpretation and enforcement more challenging.

As mentioned several times in the course of this overview, the applicable legislation is now broad and also includes the provisions and guidelines of the data protection authorities, which clarify in concrete terms the strategies that need to be adopted for each different context and type of processing, offering practical insights into concepts that at first glance seem more theoretical. Therefore, we cannot avoid conducting an analysis on the evolution of consent in the different panels of the Italian Data Protection Authority that have gathered on the subject. In 2016, Tiziana Life Sciences, a British company specialising in scientific research and the development of oncological drugs, acquired the business complex of Shar.Dna, a company founded in 2000 and subsequently declared in liquidation.

The acquisition, which took place as part of the bankruptcy proceedings, included various assets, encompassing a biobank containing genetic data and biological samples taken from approximately 11,700 individuals. These individuals were part of a community with unique genetic characteristics, due to geographical isolation that lasted for centuries. This peculiarity made the genetic data collected particularly valuable for scientific research, allowing the identification of traces of common genetics among the donors and tracing lines of descent back to the 1600s.

The samples had been provided voluntarily by the participants, who had been duly informed about the aims and purposes of the scientific research to which they would be contributing, giving their consent to the processing of their personal and genetic data. However, following the acquisition by Tiziana Life Sciences, the Italian Data Protection Authority adopted provision no. 389 of 6 October 2016[132], which ordered the temporary block of the processing of the data contained in the biobank. The measure was based on the alleged violation of the legislation on the protection of personal data, in particular for the failure to obtain a new consent from the data subjects after the change of data controller. Tiziana Life Sciences challenged the measure before the Court of Cagliari, arguing that the block imposed by the Garante was unjustified and disproportionate to the interests at stake.[133] According to the company, in fact: the processing of genetic and biological data was aimed at the same scientific purposes for which the donors had originally given their consent; the change in the

[132] Available for consultation at the following link: Garante - Provision no. 389.

[133] Manis, M. L. (2018). La Biobanca Genetica di SharDNA Spa acquistata da Tiziana Life Science PLC. Tutte le tappe della vicenda e le questioni giuridiche da risolvere. Il Sole 24 Ore.

ownership of the processing should not have entailed the need to collect consent again, since the data had been acquired in a context of continuity of scientific research. Furthermore, the provision imposed an excessive restriction on research activity, without an adequate balance between the protection of personal data and the scientific and social interest in the study of such genetic information.[134]

With ruling no. 1569/2017, the Court of Cagliari upheld the appeal of Tiziana Life Sciences, annulling the provision of the Italian Data Protection Authority. In the grounds for the judgement, the Court clarified that it is not necessary to obtain new consent every time there is a change in the data controller, provided that the original purposes remain unchanged and that the processing continues to comply with the obligations of security and protection of personal data. Furthermore, the Court held that the contested provision had not achieved an adequate balance between the protection of personal data and the scientific interest in research, emphasasing that the blocking of the processing imposed by the Data Protection Authority was an excessive and disproportionate measure with respect to the objectives of protecting the data subjects.

More recently, with order no. 28358/2023, the Italian Supreme Court has returned to the question of how consent should be expressed for registration on web platforms that deal with reputational rating, emphasising the importance of scrutiny of the transparency and comprehensibility of the algorithms used by reputational rating systems such as Mevaluate. In this context, it was clarified that the individual must be adequately informed about the functioning of the algorithm that generates the reputational evaluation. Only after acquiring this knowledge, is the individual in a position to provide informed and valid consent. In the course of a series of decisions, the Mevaluate system has faced different degrees of scrutiny regarding the legitimacy of its reputation profiling system. Specifically, it carries out an activity of quantifying the reputation value of individuals, legal persons and public and private entities, assigning them a reputation rating. This system works by using mathematical processes to process the data uploaded voluntarily by the parties concerned, who access the so-called "Mevaluate Infrastructure for Reputational Qualification" from the web, uploading documents drawn up by third parties and relating to their reputational profile. Initially, the Italian Data Protection Authority had denied authorisation for the system with provision no.

[134] Testa, G., & Marelli, L. (2018). GDPR: rischi e opportunità del nuovo regolamento europeo per la protezione dei dati personali. Science, Università Statale di Milano e Istituto Europeo di Oncologia.

488 of 24 November 2016[135]. However, upon appeal by Mevaluate, the Court of Rome, with sentence no. 5715 of 4 April 2018, partially annulled this provision, deeming the creation of reputational profiles for members to be legitimate, but confirming the illegitimacy of the so-called "counter-profiles", created by Mevaluate with regard to third parties, unrelated to the association.[136] The Garante subsequently lodged an appeal with the Court of Cassation, and the Court, with order no. 14381 of 25 May 2021, upheld the appeal, stating that the consent provided by the users of the Mevaluate platform was not valid, as insufficient information had been provided on the functioning of the algorithm used for the processing of reputational profiles. In detail, the Court held that where reference is made to the processing of personal data, consent is validly given only if freely and specifically expressed with reference to clearly identified processing. Therefore, in the case of a web platform structured for the processing of reputational profiles of individuals or legal entities, whose operation is based on the use of an algorithm designed to establish reliability scores, the requirement of awareness, necessary to guarantee free and informed consent by the user, cannot be considered satisfied if the executive scheme of the algorithm and the elements of which it is composed remain unknown or unknowable to the interested parties. For these reasons, the Court overturned the sentence of the Court of Rome with referral. In the subsequent judgement, the Court of Rome, with sentence no. 9995 of 22 June 2022, rejected Mevaluate's appeal, confirming the provision of the Data Protection Authority.[137] The Court emphasised that the functioning of the algorithm had not been made sufficiently clear to users in practice, thus preventing truly free and informed consent. However, the Court of Cassation, with Order no. 28358 of 10 October 2023, upheld Mevaluate's appeal, annulling the decision of the Italian Data Protection Authority. The Court states that consent is "validly given" only when the subject has been adequately informed about a well-defined treatment in its essential elements. In this context, the transparency of the algorithm plays a crucial role. The subject must be able to know the procedure that leads to the result and give his or her consent to it. This is in line with the principle of "free and specific" consent, which requires a detailed and unambiguous description of the algorithm. With this in mind, the Court ruled that, contrary

[135] Available for consultation at the following link: Garante - Provision no. 488.

[136] Galli, F. (2023). Reputation Rating and Algorithm Transparency: The Case of "Mevaluate". University of Bologna.

[137] Ibid.

to the opinion of the Court of Rome, Mevaluate provides an adequate explanation of the algorithm, and the parameters used for the development of the reputational rating. According to the Court, it is not necessary for the user to know the final outcome of the evaluations, which would in fact render the rating procedure itself useless, but rather the procedure that leads to these evaluations. The Court also emphasised that it is not necessary for users to understand the mathematical/computer language used, but that it is possible for experts to translate the data into a machine-readable format.[138]

In summary, the Supreme Court ruled that Mevaluate had met the requirements for "free and specific consent", since the algorithm had been described in detail and without ambiguity, allowing users to give informed consent. Therefore, the legitimacy of the Mevaluate system was confirmed, at least as far as the processing of members' reputational profiles is concerned. The "technical formula" represented by the algorithm must be accompanied by explanations that make it legible and understandable both for users and for the judge called upon to scrutinise the outcome of the evaluation carried out by the algorithm.[139]

Only through complete transparency is it possible to carry out a full evaluation of the legitimacy of the decision taken, even in a court of law, even more so in the case of reputational evaluations that have a strongly pervasive impact on the individual. This will allow the user to give valid and free consent to the processing because he or she is informed, and will allow the judge, if called upon to concretely evaluate the congruity and legitimacy of the rating operation, to examine the logic and reasonableness of the automated decision, or rather of the "rule" that governs the algorithm. [140]

The preceding pages have thoroughly examined these aspects, highlighting the ongoing phase of reassessment and redefinition of consent-not only in formal terms but also in its substantive dimension. This shift, driven by recent technological advancements, underscores the importance of equipping oneself with the necessary tools to engage with the evolving

[138] Machina Grifeo, F. (2023). Rating reputazionale sul web: il consenso deve riguardare il funzionamento dell'algoritmo. NT+ Diritto.

[139] This requirement is intrinsically linked to the right of defence of the citizen-user.

[140] Fabio, B. (2021). Rating reputazionale e trasparenza dell'algoritmo. Il caso "Mevaluate". Diritto dell'informazione e dell'informatica (Il), 2021, n. 6, Giuffrè Francis Lefebvre.

discourse on consent. The following sections will delve deeper into these emerging trends and their implications.[141]

2.2 From the illusion of free online platforms to the rise of "consent or pay" models

For years, online platforms have built their economic empire on a seemingly free model, in reality funded through the massive collection of personal data.[142] This logic has been encapsulated in a now-famous phrase stating that if one does not pay for the product, one becomes the product itself.[143] In this context, Facebook's (now Meta) decision in 2019 to quietly remove its long-standing slogan, "it's free and always will be", from its homepage can be seen as a significant turning point. This slogan, a cornerstone of the platform's marketing strategy, was replaced with the more neutral statement, "it's quick and easy": its removal, while subtle, raises important questions about the evolving business model of online platforms and their relationship with user data. It is a move that seems to acknowledge the reality that users do not receive a free service but, rather, provide valuable personal data that powers the platform's monetization strategies.

However, recent legal developments have led many companies to reconsider their approach, giving rise to models such as "consent or pay", which will be examined in detail in the following paragraphs. The current debate revolves around whether this solution genuinely constitutes a form of free and informed consent, as the model raises a series of critical issues from both an ethical and legal perspective.

Firstly, privacy is undergoing a transformation from a fundamental right into a luxury good, accessible only to those willing to pay a monthly or annual fee, depending on the desired service. This shift raises, first and foremost, a question of social justice: indeed, a fair society should ensure that economic inequalities do not translate into differential access to

[141] For recent developments on consent and a detailed analysis of the same, refer to Orlando S., (2024). Libertà e liceità del consenso nel trattamento dei dati personali. Persona e Mercato, Firenze.

[142] Digital platforms have fostered an illusion of gratuity, leading users to believe they could access services at no real cost, while in reality, the price was paid through the collection and monetization of personal data. This model became dominant with the rise of surveillance capitalism, a concept explored by Shoshana Zuboff in The Age of Surveillance Capitalism (2019), according to which digital platforms operate as extractive industries, harvesting data to predict and influence user behavior.

[143] Harris, T. et al. (2020). The Social Dilemma. Directed by J. Orlowski. Netflix.

fundamental rights.[144] The "consent or pay" model, however, would reinforce a digital divide between privileged and vulnerable users, further increasing platforms' power over the economically weaker segments of the population.

The issue is also connected to Michael Sandel's critique of the commodification of privacy[145], in which he argues that there are domains where market logic should not apply, and privacy is one of them. If the right to data protection becomes a tradable commodity, it legitimizes the principle that other fundamental rights could also be subordinated to economic capacity. The risk is the creation of a dangerous precedent in which individual freedoms are progressively monetized. Paying for privacy does not alter the underlying logic: those who cannot afford it remain tracked and profiled, while those who can pay are merely excluded from part of the surveillance, without eliminating it entirely.

The Norwegian Consumer Council published a report warning that this strategy risks turning privacy into a luxury for the few, excluding lower-income groups from the ability to protect their data.[146] The concept of "privacy-as-a-service", where users pay to avoid being tracked, has also been criticized by scholars such as Michael Veale[147] and Frederik Zuiderveen Borgesian[148], who argue that this approach undermines the principle of fairness at the core of the GDPR. Furthermore, the European Data Protection Supervisor has expressed concerns that this model could establish a market in which the right to privacy is transformed into a commodity.

As previously already mentioned, the evolution of this model has not occurred in a regulatory vacuum but in a context of increasing tension between regulators and big tech. In particular, the *Bundeskartellamt v. Meta* ruling emphasized that the processing of personal data can fall within the scope of anticompetitive practices, bridging the gap between data protection regulation and competition law. This case has prompted authorities such as the Bundeskartellamt (the German Antitrust Authority) and the European Commission to examine the implications of the "consent or pay" model also from a competition law

[144] As J. Rawls also argued in A Theory of Justice, 1971.

[145] Sandel, M. J. (2012). What Money Can't Buy: The Moral Limits of Markets. Farrar, Straus and Giroux.

[146] The Norwegian Consumer Council. (2022). Time to Ban Surveillance-Based Advertising.

[147] M. Veale is Associate Professor at UCL Laws.

[148] F. Z. Borgesian is Professor at Radboud University.

perspective. Indeed, if the alternative to providing consent is paying a high price, the choice becomes asymmetric and could be considered an abuse of dominant position by platforms holding a monopoly over the personalized advertising market.[149]

Finally, it is essential to consider the long-term implications of this model on the digital ecosystem. While the shift from an economy based solely on data collection to one incorporating subscriptions may seem like an improvement in terms of transparency, it also raises profound questions about the sustainability and fairness of the web. The vision of an open and accessible web, championed by figures such as Tim Berners-Lee[150], risks being undermined by a model in which access to high-quality digital content is contingent on users' financial capacity. This could lead to a segmented digital experience: on one side, those who can afford to pay for privacy; on the other, those who are subjected to an even more invasive level of surveillance.

Ultimately, the rise of the "consent or pay" model is not merely an economic shift but a turning point in the relationship between users, platforms, and regulators. The increasing regulatory scrutiny in Europe and ongoing legal battles will shape the future of this practice and its impact on data protection. However, the central question remains: should privacy be a universal right or a consumer good reserved for those who can afford it?[151]

2.3 The ongoing debate: antitrust and privacy in the digital economy

The analysis conducted so far shows that, although distinctive of the European approach within the global framework, the paradigm of fundamental rights does not fully explain the system of rules on consent to data processing as it has developed in the dialogue between national courts and the European Court of Justice.

It seems clear that, especially in more recent case law, the need to safeguard the integrity of the data subject's will, which is the basis for the exercise of free self-determination in terms of providing information, ends up being reconciled with the need for data circulation for the market to function properly, rather than being balanced with other fundamental rights and

[149] Podszun, R. (2020). The Consumer as a Market Player: Competition Law, Consumer Choice and Data Protection in the German Facebook Decision.

[150] Tim Berners-Lee is the British computer scientist who invented the World Wide Web in 1989 while working at CERN.

[151] Ibid. (135).

freedoms. From this point of view, the protection of personal data, as a fundamental right, is combined with market regulatory logic and takes into account the typical failures of private autonomy induced by the information asymmetries and negotiating power typical of some market relations.[152]

The complementarity between the protection of fundamental rights and the protection of the weaker party in economic relationships characterised by evident imbalance is clearly reflected in the most recent European legislation. Consider the Regulation (EU) 2022/2065 on digital services, which aims to ensure the proper functioning of the internal market for intermediary services by establishing harmonised rules that promote a secure, predictable, and trustworthy online environment (art. 1 of the aforementioned Regulation), for example through a regulation of the practices of online platform providers that may affect the decision-making processes of users.[153]

Without claiming to be exhaustive, we can also consider Regulation (EU) 2022/1925 on digital markets, which is also aimed at ensuring the fairness and contestability of so-called "gatekeepers"[154] through rules aimed at stigmatising unfair practices, including with regard to consent to the processing of personal data.[155]

In this different perspective, which therefore combines the protection of fundamental rights with the objective of rebalancing highly asymmetrical economic relations, which in turn are functional to the strengthening of the internal market, it is necessary to ask whether consent

---

[152] Gómez Alonso, A. (2024). Competition, Intellectual and Industrial Property Law. Lecture 11/24, Universidad Comillas -ICADE.

[153] This refers to enterprises providing core platform services, which serve as key access points through which business users reach end users (see Article 3, 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 (Digital Markets Act)). Under the DMA, *gatekeepers* are large digital platforms that provide core platform services such as online search engines, online social networking services, video-sharing platform services, number-independent interpersonal communication services, operating systems, cloud computing services, and online intermediation services. To be designated as a gatekeeper, a company must meet specific quantitative thresholds related to its size, user base, and impact on the internal market.

[154] Gatekeepers are large online platforms that serve as intermediaries between businesses and consumers, exerting significant control over digital markets. Under the Digital Markets Act (Regulation (EU) 2022/1925), a gatekeeper is defined as a company that meets specific criteria, such as having a strong economic position, a large user base, and an entrenched market presence in multiple EU countries. Examples include Google, Apple, Meta, Amazon, and Microsoft.

[155] According to Article 5(2) of Regulation (EU) 2022/1925, if the end user has refused or withdrawn consent given for the purpose outlined in the first paragraph, the gatekeeper may not request consent again for the same purpose more than once within a year.

to processing can become (at least in the abstract) a tool for governing the circulation of data and a counterweight to the power of data controllers.[156]

The question presents particularly critical elements if read in the light of the debate, which is also common to the consumer context, on the limits of consent in terms of the actual propensity of the data subject to exercise this instrument of voice or, on the contrary, to develop a supine attitude to an authorising consent devoid of any real function of governance.[157]

Disregarding these latter solicitations, according to approaches that are comparable to consumer regulation, the European legislator reinforces the role of consent through a solid apparatus of information obligations, aimed at guaranteeing the full awareness of the consenting interested party and at reducing, at least in part, the asymmetry of power in the relationship with the owner.[158]

However, as already mentioned above, it is clear that, far beyond the paradigm of consumer protection, this information is interpreted, in the perspective of the Court of Justice, according to a principle of effectiveness (of the protection and of the will of the interested party), whereby the information must not only be given to the "weak" subject and not only received by him but even "assimilated", so as to affect not only in the abstract but also in practice the decision-making process of the interested party.[159] In this evolution we can see an attempt to contaminate the traditional schemes of consumer protection with the demands underlying the protection of fundamental rights. However, the question of the actual suitability of the mechanisms aimed at stimulating an active consensus to overcome the limits induced by an excess of information and consultation of the interested party, highlighted by behavioural sciences, remains unanswered.[160]

---

156 Filpi, G. (2022). Il rapporto tra data protection e diritto antitrust alla luce del caso "Facebook Germany": Analisi e prospettive future.

157 B.W. Schermer, B. Custers, and S. van der Hof, (2014). The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection, Ethics and Information Technology. See also I.A. Caggiano, (2018). Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali, in Osservatorio di diritto civile e commerciale.

158 European Data Protection Board, Guidelines 5/2020 on Consent under Regulation (EU) 2016/679, 4 May 2020, p. 16.

159 Court of Justice of the European Union, 11 November 2020, Orange Romania SA v. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, C-61/19, para. 46.

160 See N. Richards and W. Hartzog, (2019). The Pathologies of Digital Consent, Washington University Law Review, where the authors argue that consent can serve as an effective control mechanism in the current digital

An even more problematic contamination, between instances of protection of fundamental rights and objectives of correcting asymmetries of power in the internal market, seems to emerge where the role of consent is called into question in the context of relationships characterised by an "evident imbalance" between the holder and the interested party. According to Recital 43 of the Regulation, "to ensure the freedom to give consent, it is appropriate that consent not constitute a valid legal basis for the processing of personal data in a specific case, if there is a clear imbalance between the data subject and the data controller, especially when the data controller is a public authority and this therefore makes it unlikely that consent was given freely in all the circumstances of that specific situation".[161]

It should not be overlooked that this assessment of appropriateness, although relevant for the purposes of interpreting the GDPR, has not been incorporated into Article 7 on the subject of consent (unlike the rest of the recital, which is instead reflected in paragraph 4 of the same article).

At the same time, even if only on an interpretative level, this reference opens a clear breach in the system, apparently distancing the fate of the data subject's self-determination (incompatible with an asymmetrical structure) from that of the consumer decision (compatible with the asymmetrical nature of the commercial relationship). Is the consent of the interested party therefore structurally unsuitable for governing the circulation of data in the context of relationships characterised by "evident imbalance"? Is the reference to public authority, contained in Recital 43, sufficiently meaningful to suggest an equal concern for

environment if its request is infrequent, if the negative consequences of a poor choice are immediately apparent, and if the data subject has clear incentives to make a serious and informed decision.

From this perspective, it is worth noting that even in recent European legislation, while ensuring the lawfulness of data processing through a valid legal basis remains essential, there is a growing tendency to tailor protective mechanisms based on the impact that regulated entities' activities may have on fundamental rights. A key role in this regard is played by risk assessment tools, which require operators to consider, among other factors, the potential negative effects-both actual and foreseeable-on the exercise of fundamental rights, including human dignity (Article 1 of the Charter), the right to respect for private and family life (Article 7 of the Charter), the protection of personal data (Article 8 of the Charter), freedom of expression and information, including media freedom and pluralism (Article 11 of the Charter), non-discrimination (Article 21 of the Charter), the rights of the child (Article 24 of the Charter), and a high level of consumer protection (Article 38 of the Charter), as outlined in Article 34 of Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act). This additional obligation applies exclusively to providers of very large online platforms and very large online search engines for the management of systemic risks. It complements the broader framework established by the GDPR, which imposes general obligations on data controllers regardless of their size or the impact of their activities on fundamental rights, except for possible adjustments left to national legislation or private regulation (see Recital 13 and Article 40 GDPR).

[161] Recital 43 of GDPR.

"private authorities" which, precisely in the context of the digital economy, preside over relationships characterised by "evident imbalance"?

The Court of Justice recently dealt with this issue in the *Meta* case, already mentioned and which will be developed shortly.[162] Anticipating an important passage, the Court, aligning itself with the conclusions set out by the AG, has partly repaired the apparent fracture between informational self-determination and consumer decision-making outlined above. In the case in question, the European judge in fact excluded that the aforementioned Recital 43 should be interpreted as tracing an irreducible incompatibility between free consent and evident imbalance in the relationship between the owner and the data subject. To this end, with a formula that recalls the approach of the same Recital on the subject of conditioning consent, it has identified in the evident imbalance (in the case in question, the dominant position) an important element in assessing the freedom of consent: important but not exclusive, nor decisive. In the Court's view, as with consumer relations, a space for informative self-determination of the interested party is therefore preserved even in the context of highly asymmetrical relations, provided that other and more meaningful guarantees of freedom of consent exist. In this sense, the parameters already provided for by the Regulation are recalled, with particular regard to the specificity of consent with respect to individual processing and the availability, for the data subject, of "equivalent alternatives" not accompanied by data processing, "if necessary, against adequate compensation"[163] and with the possibility of revoking consent without prejudice.[164]

---

[162] Court of Justice of the European Union, 4 July 2023, Meta Platforms, C-252/21. The case was recently concluded with a judgment by the Court of Justice. In an earlier stage, the German Federal Competition Authority had prohibited Meta Platforms from making the use of its social network by private users residing in Germany conditional on the processing of certain personal data under its general terms and conditions.
Following this decision, Meta introduced new terms explicitly stating that users consent to receiving personalized advertisements - based on the processing of their personal data - as an alternative to paying for access to Facebook's services.

[163] The Court of Justice of the European Union stated in *Meta Platforms*, C-252/21, para. 150, that users must have the freedom to individually refuse consent for specific data processing operations that are not necessary for the performance of a contract. This refusal should not require them to forgo access to the online social network service entirely. Consequently, users should be offered an equivalent alternative, which, if necessary, may involve an appropriate fee, but without being subject to the same data processing operations.

[164] The Court of Justice of the European Union, in Meta Platforms, C-252/21, paras. 144-150, appears to suggest that such 'detriments' cannot be equated with the 'appropriate fee' mentioned in its reasoning. The Court frames this fee as compatible with the existence of "equivalent alternatives", implying that the financial cost itself does not constitute an undue burden on users exercising their choice regarding data processing.

The asymmetry of digital relationships, as well as that of commercial relationships, is therefore a relevant factor in determining the tools for protecting the interested party and guaranteeing his fundamental rights.

However, as in European law on unequal relationships, it is not the allocation of economic power alone that induces the legal system to react, nor to erect preventive barriers to the exercise of one's autonomy, but rather the abuse of that power through practices that hinder the free choice of the weaker party. Since, in the context of data protection, this free choice is also the exercise of a fundamental right, the practice is evaluated more rigorously (for example, requiring active participation by the weak party, not normally expected by the consumer) and the operator is required to adopt an economic model that is compatible with the exercise of consent inspired by the principle of effectiveness. From this point of view, it is no coincidence that the issue of "equivalent alternatives" to the service combined with the processing of personal data not necessary for the execution of the contract has once again caught the attention of the European legislator in the Regulation on digital markets regarding unfair practices by *gatekeepers*.[165]

The reference to the effectiveness of consent is not only valid for configuring the aforementioned "equivalent alternatives" without the processing of data that can be freely refused, but also for guaranteeing substantial space for its revocation, a necessary complement to the fundamental right to informational self-determination. The Court of Justice recently dealt with this issue in the *Proximus* case[166], as an operator of publicly accessible telephone directory enquiry services, built in collaboration between several operators through the sharing of data transmitted by customers who had consented to publication. In such a context, the asymmetrical relationship between the individual concerned and the individual data controller is further complicated by the circulation of data between the various operators. The presence of multiple data controllers, even if

[165] Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act), Recitals 36 and 37, emphasizes that gatekeepers must not unfairly undermine the contestability of core platform services. They are required to allow end users to freely choose whether to accept data processing and access practices, ensuring the availability of an equivalent but less personalized alternative. The use of core platform services or specific functionalities must not be conditioned on the user's consent. However, gatekeepers retain the possibility to process personal data or require registration-based access under the legal bases outlined in Article 6(1)(c), (d), and (e) of Regulation (EU) 2016/679 (GDPR), but not under Article 6(1)(b) and (f). Moreover, the less personalized alternative must not differ in nature or be of lower quality compared to the service offered to consenting users, unless such a reduction in quality directly results from the gatekeeper's inability to process personal data or enforce registration-based access.

[166] CJEU, Case C-129/21, Proximus NV v. Gegevensbeschermingsautoriteit, Judgment of 27 October 2022.

communicated to the consenting data subject, increases the asymmetry of power in the relationship between data controller and data subject and becomes an obstacle to the effectiveness of informational self-determination, to be exercised with each of the data controllers. Applying the principle of effectiveness, the Court of Justice has mitigated this asymmetry by recognising a specific obligation for the recipient provider of the revocation request to forward the same request to the various providers and search engines.[167]

For consent and its withdrawal to be tools for governing the circulation of personal data in the context of asymmetrical relationships, the data controller has an organisational burden aimed at containing, at least in part, the effects of that asymmetry. So, if on the one hand, European case law continues to see the consent of the data subject as an important pillar of the protection of fundamental rights affected by the circulation of data, on the other hand, there is a growing emphasis in European legislation and case law on complementary means of protection, aimed at combatting unfair practices in the context of asymmetric economic relations and therefore at guaranteeing the proper functioning of the market even before, or at least together with, the protection of fundamental rights.

This approach, far from weakening the distinctive feature of the European model based on the protection of fundamental rights, tends to strengthen it by leveraging a complementarity of protections that is entirely consistent with the principle of effectiveness.[168]

Moreover, while instruments designed to correct power asymmetries help create conditions for the exercise of freedom, they do not truly guarantee that individuals have read, understood, and fully assimilated the information, nor that they have made a genuinely informed decision, it has also been shown that a granular and systematic search for informed consent, as an exercise in fundamental and free self-determination, does not lead to concretely appreciable results in terms of individuals' participation in data governance.[169]

In a sense, this is demonstrated by the recent research of the legislator to favour forms of support for the exercise of rights based on delegation to collective organisations, invested

---

[167] This follows from Article 19, which establishes a similar obligation in cases where data deletion is requested, except when such deletion would require a disproportionate effort. See Court of Justice of the EU, 27 October 2022, Proximus NV, C-129/21.

[168] Cafaggi, F. (2008). Judicial and Administrative Enforcement in Consumer Protection: The Way Forward.

[169] Neil Richards and Woodrow Hartzog, (2019). The Pathologies of Digital Consent, Washington University Law Review, op. cit., pp. 1476 et seq.; B.W. Schermer, B. Custers and S. van der Hof, (2014). The Crisis of Consent, in Ethics and Information Technology.

not with the mere task of administering economic rights connected to the enjoyment of fundamental rights but with the very act of giving consent as the beating heart of informative self-determination.[170] Having accepted the complementarity between different regulatory approaches, it is a question of understanding the professional practices of large operators aimed at guaranteeing the effective participation of the individual in the governance of data, including through the provision of consent to the processing of personal data.

From this point of view, behaviourist readings that lead to a preference for more selective information, focused on determining profiles and a non-obsessive search for consent, are very useful. Consent is not intended as a form of authorisation and endorsement of unilaterally determined treatments, but as effective and truly conscious participation.[171]

In terms of regulation, this approach, only partially emerging in the most recent initiatives, would lead to the calibration of information obligations and involvement of the data subject according to the risk of impact on the fundamental rights of the individual, the nature of the data processed (e.g. whether it belongs to special categories pursuant to art. 9 GDPR), the purpose of the processing and the possibility of secondary uses, the effective existence of a space for revocation and/or withdrawal of the processing. An application of current law that respects the principles of effectiveness and proportionality could lead to more effective outcomes in the same perspective of a high level of protection of fundamental rights.[172]

In the following pages, we will see a recent attempt at the practical application of these aspects.

[170] Regulation (EU) 2022/868 of 30 May 2022, relating to European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), Recital 31: Data cooperatives aim to achieve several objectives, primarily strengthening the position of individuals so they can make informed choices before consenting to the use of their data. These cooperatives work to influence the terms and conditions set by data user organizations, which govern the use of data, offering better choices to individual members of the group. They also seek solutions to conflicting positions regarding data usage among group members when the data concerns multiple individuals within the group. It is important to note that under Regulation (EU) 2016/679, data subject rights are personal and cannot be waived. Data cooperatives may also serve as a useful tool for individual businesses and SMEs, which often have similar levels of knowledge about data sharing as individual data subjects.

[171] N. Richards and W. Hartzog. (2019). The Pathologies of Digital Consent, Washington University Law Review.

[172] Iamiceli, P. (2024). Consenso al trattamento e giurisprudenza europea. Libertà e liceità del consenso nel trattamento dei dati personali. Firenze, Persona e Mercato.

2.4 The implications of Case C-252/21

In February 2019, the German competition authority[173] imposed restrictions[174] on Facebook's processing of users' personal data, concluding that the company engaged in exploitative business practices under Section 19(1) GWB[175], a provision largely corresponding to Article 102 TFEU[176]. The BKA determined that Facebook had abused its dominant position by requiring users to accept terms and conditions that enabled the collection of personal data beyond its own platform - specifically from its affiliated services and third-party websites -and by merging this data with users' Facebook profiles[177], and by leveraging this extensive data aggregation to a degree that competitors could not replicate.[178] The authority asserted that consent could not be deemed valid if it was a prerequisite for accessing Facebook's services.[179] Moreover, it was linked the lack of valid consent to Facebook's market dominance and the absence of alternative social networking platforms, and the authority held that processing personal data without a lawful basis under the General Data Protection Regulation constituted an exploitative abuse of Facebook's dominant position.[180]

---

[173] The German Competition Authority, also known as the *Bundeskartellamt* (BKA), is responsible for enforcing competition law in Germany.

[174] If the question arises as to whether the German competition authority may detect a violation of the GDPR and whether it has the power to ascertain such a violation, the answer is unequivocally affirmative: if a violation results in a competitive advantage, it is deemed unlawful (as also confirmed by the Italian Supreme Court in plenary session in the *fideiussioni omnibus* case, Judgment No. 41994 of 30 December 2021).

[175] The Act against Restraints of Competition (*Gesetz gegen Wettbewerbsbeschränkungen*, GWB) is the primary legal framework governing competition law in Germany.

[176] Article 102 of the Treaty on the Functioning of the European Union (TFEU) prohibits the abuse of a dominant position within the internal market or in a substantial part of it, insofar as it may affect trade between Member States. Such abuse may include imposing unfair purchase or selling prices, limiting production, markets or technical development to the detriment of consumers, or applying dissimilar conditions to equivalent transactions, thereby placing certain trading parties at a competitive disadvantage.

[177] The *Bundeskartellamt* refers to third-party sources as services owned by Facebook, such as WhatsApp and Instagram, as well as third-party websites that "embedded Facebook products such as the 'like' button or a 'Facebook login' option or analytical services such as 'Facebook Analytics'".

[178] Satariano, A. (2020). Facebook Loses Antitrust Decision in Germany Over Data Collection. The New York Times.

[179] German Competition Authority (n. 1).

[180] Podszun, R. (2020). The Consumer as a Market Player: Competition Law, Consumer Choice and Data Protection in the German Facebook Decision.

Following the appeal by Facebook, the Düsseldorf Higher Regional Court decided to suspend the enforcement of the Germany competition authority's order as part of *interim* proceedings and simultaneously referred a request for a preliminary ruling to the European Court of Justice.[181] Among the various legal questions submitted, the referring court specifically sought clarification on whether the consent granted by users of an online social networking

platform to an operator holding a dominant market position could still be regarded as freely given within the framework of the GDPR.[182]

In its ruling[183], the ECJ established that the mere fact that an online platform operator enjoys a dominant position in the market does not, in itself, preclude the possibility of obtaining valid user consent in accordance with Article 4(11) GDPR.[184] Nevertheless, the Court underscored that such a dominant position constitutes a relevant factor when assessing whether users have indeed provided consent voluntarily and without undue external pressure.[185] In this regard, the Court highlighted that such a situation must be considered when assessing whether the user of that network has provided valid and, in particular, freely given consent, as it may impact the user's freedom of choice.[186] In particular, the user might face difficulties in refusing or withdrawing consent without suffering any disadvantage, as highlighted in Recital 42 of the GDPR.[187]

---

[181] Volmar, M. N., & Helmdach, K. O. (2018). Protecting consumers and their data through competition law? Rethinking abuse of dominance in light of the Federal Cartel Office's Facebook investigation. European Competition Journal.

[182] Court of Justice of the European Union, 4 July 2023, Meta Platforms Inc. v. Bundeskartellamt, C-252/21, para. 140.

[183] In this regard, the lack of an inquiry into the impact of competitive dynamics appears questionable, as the ECJ does not address the causal link between the violation and the harm to the market. Moreover, it is also debated whether the mere verification of a regulatory violation can exempt the authority from the requirement to provide strict proof of the existence of a causal link.

[184] Court of Justice of the European Union, 4 July 2023, Meta Platforms Inc. v. Bundeskartellamt, C-252/21, para. 147.

[185] D'Amico, A. S. (2023). Market Power and the GDPR: Can Consent Given to Dominant Companies Ever Be Freely Given? Utrecht University School of Law Research Paper.

[186] Podszun, R., & Marsden, P. (2020). Restoring balance to digital competition – Sensible rules, effective enforcement. Konrad-Adenauer-Stiftung e. V.

[187] Court of Justice of the European Union, 4 July 2023, Meta Platforms Inc. v. Bundeskartellamt, C-252/21, para. 148.

The ECJ further elaborated that a company's market dominance may create an inherent power imbalance between the service provider and its users, potentially leading to the imposition of contractual terms and conditions that exceed what is strictly necessary for the performance of the underlying contract.[188] Accordingly, the Court clarified that, in order for consent to meet the requirements of validity under the GDPR, individuals must retain the genuine ability to refuse the processing of their personal data when such processing is not essential to fulfilling the contractual obligations of the service provider. Moreover, users should not be denied access to an equivalent version of the service solely due to their refusal to grant consent, although the Court acknowledged that, under certain conditions, access to such an alternative service could be subject to an appropriate fee.[189]

In the aftermath of the Meta judgment, the European Data Protection Board (EDPB) took decisive action in response to ongoing concerns regarding Meta's data processing practices.[190] In October 2023, at the request of the Norwegian Data Protection Authority[191], the EDPB issued an urgent binding decision addressing Meta's reliance on specific legal bases for behavioral advertising.[192]

In this decision, the EDPB unequivocally determined that Meta could no longer justify the processing of personal data for targeted advertising purposes on the grounds of either contractual necessity or legitimate interest. Given Meta's persistent failure to comply with the GDPR, the EDPB concluded that immediate and definitive enforcement measures were required and accordingly instructed the Irish DPA[193] to impose a prohibition on the processing of personal data collected for behavioural advertising purposes under the legal basis of contract and legitimate interest.

In response to growing regulatory scrutiny, Meta introduced a new subscription-based model, commonly referred to as the "pay-or-okay" system, in November 2023.[194]

---

188 Court of Justice of the European Union, 4 July 2023, Meta Platforms Inc. v. Bundeskartellamt, C-252/21, para. 149.

189 Seufert, E. (2023). What Is an "Appropriate Fee"? Mobile Dev Memo.

190 Craddock, P. (2024). Op-Ed: A Critical Analysis of the EDPB's "Pay or Consent" Opinion.

191 The Norwegian Data Protection Authority is also known as Datatilsynet.

192 European Data Protection Board, Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Article 66(2) GDPR), 27 October 2023.

193 The Irish Data Protection Authority is also known as the Data Protection Commission (DPC).

194 "Meta and Instagram to Offer Subscription for No Ads in Europe", 30 October 2023.

Users of Facebook and Instagram were presented with a notification outlining a binary choice between two distinct alternatives:

- Subscription for an ad-free experience: users could opt to pay a monthly fee, starting at €12.99 (inclusive of applicable taxes), in exchange for access to Facebook and Instagram without advertisements. Under this option, Meta would refrain from utilizing their personal data for targeted advertising purposes.
- Continued free usage with ads: alternatively, users could choose to continue using Facebook and Instagram at no monetary cost, with the understanding that their personal information would be processed to deliver personalized advertisements.[195]

Effectively, this framework compels users to decide between granting Meta explicit consent for behavioral advertising, paying a subscription fee to avoid data-driven ad targeting, or discontinuing their use of the platform in favor of an alternative service provider.[196]

The introduction of this model has sparked significant debate, particularly regarding its compliance with various aspects of European data protection, consumer protection, and competition law.[197] Several complaints have been lodged before national authorities, including cases brought before the Spanish Data Protection Authority[198] and the Austrian DPA[199] by the advocacy group None of Your Business (Noyb).[200]

Noyb has argued that the pay-or-okay model violates the GDPR, while the European Consumer Organisation[201] has submitted a separate complaint, contending that Meta's approach is inconsistent with the Unfair Commercial Practices Directive[202].

---

[195] Lawler, R. (2023). Ad-Free Instagram and Facebook Is Here – and It's Expensive. The Verge.

[196] Witt, A. C. (2021). Excessive data collection as a form of anticompetitive conduct – The German Facebook case. The Antitrust Bulletin.

[197] Including comprehensive complaints filed by the privacy organization NOYB and the consumer organization BEUC.

[198] Complaint filed on behalf of the complainant by Jorge García Herrero. The Spanish Data Protection Authority is also known as the Agencia Española de Protección de Datos (AEPD).

[199] The Austrian Data Protection Authority is also known as the Österreichische Datenschutzbehörde (DSB).

[200] In November 2023, NOYB filed a complaint with the Austrian DPA against Meta under Article 77(1) GDPR.

[201] The European Consumer Organisation (BEUC) is an umbrella group representing 45 independent consumer organizations from 31 European countries.

[202] The Unfair Commercial Practices Directive (2005/29/EC) aims to protect consumers from unfair business practices in the internal market. It prohibits misleading and aggressive commercial practices and establishes

Moreover, Meta's decision to adopt this model was, at least in part, a direct response to the competition law proceedings initiated by the German Federal Cartel Office.[203] This raises critical questions about whether the pay-or-okay system adequately addresses the competition concerns identified by the BKA or whether it instead introduces new risks of anticompetitive outcomes. The legal reasoning developed in the Meta case has also influenced broader regulatory developments, as evidenced by the inclusion of a similar provision in the Digital Markets Act[204], which imposes additional obligations on designated gatekeepers regarding their data processing practices. In March 2024, the European Commission launched a formal investigation to assess the extent to which Meta's implementation of the pay-or-okay model complies with the DMA.[205]

The implementation of Meta's pay-or-okay model brings into play two key regulatory frameworks: the General Data Protection Regulation and the ePrivacy Directive.[206]

The GDPR governs the processing of personal data and mandates that data controllers establish a valid legal basis for any data processing activities. Meanwhile, the ePD introduces additional requirements specifically related to the use of tracking technologies. Under these combined regulatory provisions, as we have already discussed in detail in the previous sections, websites and online platforms operating within the EU must obtain user consent before engaging in tracking activities that are not deemed strictly necessary.[207] This requirement extends to targeted advertising, which falls squarely within the category of non-essential data processing.[208]

---

rules for the protection of consumers against practices that distort their economic behavior, ensuring a high level of consumer protection across the EU.

[203] Fabbio, P. (2019). Il diritto della concorrenza in Germania: osservazioni e valutazioni in prospettiva europea. Orizzonti del diritto commerciale, fascicolo 3/2019.

[204] See note 151.

[205] European Commission, (2024). Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act, Press Release IP/24/1689 of 25 March 2024. Moore, M., & Tambini, D. (2018). Digital Dominance: The Power of Google, Amazon, Facebook, and Apple.

[206] European Parliament and Council, (2002). Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L 201/37.

[207] Directive on privacy and electronic communications, (n 19), Article 5(3), OJ 2002 L 201/37.

[208] Santos, C., Bielova, N., & Matte, C. (2020). Are Cookie Banners Indeed Compliant With the Law? Deciphering EU Legal Requirements on Consent and Technical Means to Verify Compliance of Cookie Banners. Technology and Regulation.

Determining whether consent is required in a given scenario necessitates an assessment of the specific purpose for which each tracking mechanism is deployed within a website or application.[209] In the context of online behavioral advertising, GDPR enforcement actions have consistently affirmed that valid user consent constitutes the only acceptable legal basis for such data processing activities. This principle has been reaffirmed in multiple decisions against Meta, issued by regulatory authorities and judicial bodies across Europe, including in Germany, Ireland, and Norway, as well as through binding decisions by the European Data Protection Board and judgments of the Court of Justice of the European Union[210].

Consent, as defined under the GDPR, must satisfy a series of stringent requirements: it must be obtained prior to data processing, given freely, specific to a clearly defined purpose, informed, unambiguous, presented in a readable and accessible manner, and easily revocable.[211]

In the context of Meta's pay-or-okay model, the most contentious requirement is that of *freely given* consent. This paragraph also aims to examine whether the model aligns with this fundamental principle under the GDPR, taking into account the specific legal standards articulated by data protection authorities in relation to such monetized consent frameworks.[212]

Indeed, there is considerable legal ambiguity surrounding the question of whether consent obtained through Meta's pay-or-okay model can be considered truly *freely given* as required under Article 4(11) of the GDPR, and further elaborated in Article 7(4) and Recital 42. For consent to be valid, individuals must be able to make a voluntary and genuine choice regarding the processing of their personal data, without being subjected to undue influence, coercion, or adverse consequences for refusing consent.[213] The notion of free consent is

[209] Article 29 Working Party, (2012). Opinion 04/2012 on cookie consent exemption (WP 194, 7 June 2012).

[210] Among the most relevant cases is the Facebook and WhatsApp case (Case C-252/21, European Court of Justice), which addresses critical issues related to user consent, data sharing between companies, and the transparency of privacy policies. This case highlights the challenges of ensuring compliance with the GDPR in the context of large-scale data processing and cross-platform integration.

[211] GDPR (General Data Protection Regulation), Articles 4(11),7.

[212] This model is also referred to as *cookie paywalls*. See: Morel, V., Santos, C., Lintao, Y., & Human, S. (2022). Your Consent Is Worth 75 Euros A Year – Measurement and Lawfulness of Cookie Paywalls. 21st Workshop on Privacy in the Electronic Society (WPES '22), Los Angeles, CA, USA, November 2022.

[213] Kerber, W. (2022). The German Facebook Case: The Law and Economics of the Relationship Between Competition and Data Protection Law.

undermined if users feel pressured into agreeing, lack viable alternatives, or face significant disadvantages - such as excessive costs - if they choose not to provide consent.[214]

The European Data Protection Board has explicitly warned against practices that erode user autonomy, emphasizing that any form of inappropriate pressure or influence that limits an individual's ability to exercise free will results in invalid consent. A particularly contentious issue arises when access to an online service is conditioned on the acceptance of non-essential tracking technologies, as such requirements may, in certain instances, compromise users' freedom of choice and ultimately affect the legitimacy of their consent.[215]

According to the EDPB's guidelines, the concept of freely given consent is built upon four fundamental principles: the absence of power imbalance, unconditionality, granularity, and non-detriment. In this section, we argue that Meta's pay-or-okay model fails to meet these criteria. Specifically, the model presents an inherent imbalance of power between the user and the platform, conditions access to the service on consent, lacks sufficient granularity in how consent is structured, and imposes financial or functional detriment on those who refuse. Collectively, these factors indicate that the consent obtained under this framework is neither free nor lawful within the meaning of Article 6 of the GDPR.[216]

The EDPB has consistently maintained that when a significant imbalance of power exists between a data controller and a data subject, consent cannot be considered freely given.[217] In the case of Meta's model, such an imbalance appears evident. Several factors contribute to this dynamic, including the company's overwhelming market dominance and the strong network effects that create a *lock-in effect*, making it difficult for users to switch to alternative platforms. Additionally, Meta's monopoly extends to general-purpose social networking platforms, distinguishing it from services with a more specific focus, such as LinkedIn (professional networking) or TikTok (younger demographic). These elements reinforce a

---

[214] The EDPB Guidelines 05/2020 on consent highlight additional examples of situations that may undermine valid consent, such as deception, intimidation, coercion, or significant negative consequences for the data subject in case of refusal (para. 47). They also refer to cases where consent is compromised due to compulsion, pressure, or a lack of genuine free choice (para. 24). See: EDPB, (2020). Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, Adopted 4 May 2020.

[215] Commission Nationale de l'Informatique et des Libertés, (2022). Cookie walls: la CNIL publie des premiers critères d'évaluation, 16 May 2022.

[216] D'Amico, A. S., Pelekis, D., Santos, C., & Duivenvoorde, B. (2024). Meta's Pay-or-Okay Model: An Analysis Under EU Data Protection, Consumer, and Competition Law. Utrecht University School of Law Research.

[217] Recital 43 of GDPR.

structure of dependency, suggesting a subordinate relationship between users and the platform.[218]

Under Article 7(4) and Recital 43 of the GDPR, consent is presumed *not* to be freely given when the provision of a service is conditional on the disclosure of personal data that is unnecessary for the service itself.[219] This principle also applies to tracking technologies: if cookies or similar mechanisms are not essential to the core functionality of a service and serve primarily to benefit the website operator, users must have a genuine choice to refuse them.[220]

Applying this to Meta's *pay-or-okay* model, access to the platform is contingent on users consenting to data processing that is not strictly necessary for the core service-namely, targeted advertising. Since advertising has been ruled as non-essential to the fundamental provision of social networking services, it follows that such consent is effectively coerced. As a consequence, the burden falls on Meta, as the data controller, to prove that users' consent is truly voluntary. In practice, this means that consent must be unbundled from contractual obligations-such as access paywalls-ensuring a clear distinction between the acceptance of data processing and the provision of services, in line with Article 7(2).

The EDPB has further emphasized this principle, asserting that the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract. This concern is echoed by NOYB, which argues that linking consent to a payment mechanism effectively transforms the fundamental right to privacy into a transactional commodity-forcing users to "purchase" their right to data protection from the controller. This perspective aligns with the rationale articulated by the EDPB in multiple decisions, including Binding Decision 3/2022[221], which states that the GDPR, in line with EU primary law, regards personal data as a fundamental right tied to the

[218] Zeno-Zencovich, V. (2019). Do Data Markets Exist? Medialaws.

[219] EDPB, (2020). Guidelines 05/2020 on consent under Regulation 2016/679, para. 39.

[220] According to the guidance from the Article 29 Working Party, if certain cookies are not essential for providing the website service but only offer additional benefits to the website operator, the user must be given a genuine choice regarding those cookies. See: Article 29 Working Party, (2013). Working Document 02/2013 providing guidance on obtaining consent for cookies (WP 208, 2 October 2013).

[221] For further details, see the EDPB Binding Decision (2022), available at: EDPB - 03/2022. This decision reversed the more permissive approach previously taken by the Irish Data Protection Commission.

dignity of the data subject, rather than as a commodity that individuals can relinquish through contractual agreements.[222]

Data subjects should retain the freedom to selectively consent to specific processing purposes rather than being required to accept a bundled set of purposes. Recital 43 of the GDPR establishes that consent cannot be deemed freely given if individuals are not provided with the option to grant separate consent for different processing activities. Similarly, Recital 32 further clarifies that consent must encompass all processing activities related to the same purpose or purposes. In cases where processing involves multiple purposes, consent must be obtained for each of them. In the context of Meta's *pay-or-okay* model, uncertainties arise regarding whether users who opt for the paid alternative will still be subject to tracking and, if so, for what specific purposes beyond advertising. Likewise, for those who do consent to targeted advertising, it remains unclear whether their data may also be processed for additional, undisclosed purposes.[223]

The concept of *detrimental consent* is particularly relevant here. According to Recital 42 of the GDPR, consent is invalid if the data subject cannot refuse or withdraw it without suffering detriment or negative consequences. The EDPB has stressed that controllers bear the burden of proving that withdrawing consent does not impose any costs or disadvantages on the user.[224] In its complaint against Meta, NOYB highlighted two primary disadvantages for users: first, rejecting consent requires significantly more effort than granting it, as users must enter payment details or set up an Apple or Google account for in-app purchases on iOS and Android. Second, users must navigate through multiple windows and banners before reaching the page where they can actually withdraw consent. Moreover, withdrawing consent ultimately forces the user to either subscribe and pay a monthly fee or delete their account altogether-effectively eliminating the possibility of free withdrawal.[225]

---

[222] EDPB, (2022). Binding Decision 3/2022 on the dispute submitted by the Irish SA regarding Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), Adopted 5 December 2022, para. 101.

[223] Kerber, W., & Zolna, K. K. (2022). The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law. European Journal of Law and Economics, 34 pages.

[224] EDPB, (2020). Guidelines 05/2020 on consent under Regulation 2016/679, para. 42.

[225] Hoefling, S. (2022). The German Facebook Case - Alternative Membership Models as An Approach? 54 pages. Posted: 4 January 2022. Date Written: 6 September 2021.

Regulators across Europe have taken diverging positions on the *pay-or-okay* approach.[226] Some data protection authorities, including those in Spain, France, Denmark, and Austria, have adopted generally permissive stances, provided that specific legal conditions are met. These authorities have emphasized the need for:

1. A *reasonable and fair alternative* that does not involve tracking for targeted advertising. However, DPAs differ on what constitutes an appropriate alternative - some argue that the service offered should be largely similar, while others insist on *genuine equivalence*, meaning that paying users should not receive significantly more content than those who consent to data processing.[227]
2. An assessment of *potential power imbalances* in determining whether an alternative is truly reasonable. The French DPA, for instance, notes that if a website provides exclusive content or functions as an essential service, this could undermine the voluntariness of consent.
3. *Granularity of consent*, requiring that users be able to choose ("yes" or "no") for each specific processing purpose separately.[228]
4. A *reasonable price* for the paid alternative.
5. Restrictions ensuring that, when users pay, their personal data is processed only as strictly necessary.[229]
6. Clear and transparent *user information*, including the disclosure that refusing cookies may limit or restrict access to the website or its services.[230]

This ongoing debate underscores the fundamental tension between business models reliant on targeted advertising and the GDPR's requirement that consent be truly voluntary, informed, and free from coercion.

---

[226] Recently, the Dutch, Norwegian, and Hamburg DPAs have sought an opinion from the EDPB regarding this approach, while the Irish DPA is expected to publicly disclose its position soon.

[227] Datenschutzkonferenz, (2023). Evaluation of Pur-Subscription Models on Websites, Resolution of the Conference of Independent Data Protection Supervisory Authorities of the Federal and State Governments, 22 March 2023.

[228] As also mentioned by Datatilsynet (the Norwegian Data Protection Authority), responsible for overseeing the implementation of data protection laws in Norway. See: Österreichische Datenschutzbehörde, Case 2023-0.174.027, decided on 29 March 2023.

[229] Datatilsynet, (2023). Brug af Cookie Walls, 20 February 2023.

[230] See also: Agencia Española de Protección de Datos, (2024). Guía sobre el uso de las cookies, January 2024.

In December 2023, as a response to the European Commission's cookie pledge, the European Data Protection Board clarified that it is not possible to determine *in abstracto* whether the availability of a paid alternative to a service that relies on tracking ensures valid consent for processing user data for advertising purposes. Instead, it emphasized the necessity of a case-by-case assessment to establish whether consent for advertising meets legal validity requirements, identifying key criteria to be considered. These include ensuring that consent is informed - where details about alternative models or services may be a relevant factor in assessing validity - along with verifying whether an additional service option beyond both a tracking-based and a paid service is offered, such as one utilizing a less intrusive form of advertising like contextual ads. Additionally, the ability of the data subject to make a genuine choice among the different options presented is considered essential.[231]

In the specific case of Meta's business model, the informed consent requirement plays a fundamental role in determining whether users' consent is truly voluntary. This includes the obligation to provide details about an equivalent alternative offer, assess the appropriateness of the fee charged, and clarify the specific purposes for which personal data is processed. In this regard, Noyb's complaint argued that Meta's model breaches the requirement of informed consent, alleging that the available choice does not sufficiently inform users about whether they will still be tracked after opting for the paid version, as well as the specific purposes and legal basis for such processing.[232] Furthermore, empirical research on consent suggests that users generally do not read consent requests or privacy policies, raising concerns that mandated disclosures alone may fail to ensure genuinely informed decision-making.[233]

Although the fee for a tracking-free alternative should be reasonable, neither the EDPB nor any Data Protection Authority has established clear metrics, factors, thresholds, or contextual considerations to assess the appropriateness and fairness of such pricing. Consequently, DPAs hold broad discretionary power in this regard, effectively assuming a "price regulator" role, despite the lack of explicit criteria defining what constitutes a reasonable fee.

This means that determining the acceptability of Meta's pricing will ultimately require a case-by-case analysis, varying across different countries and, accordingly, for each individual user.

---

[231] Nettesheim, M. (2024). EU Data Protection Law and Pay-or-Consent Business Models.

[232] Noyb, (2023). Complaint to the Austrian DPA against Meta under Article 77(1) GDPR, November 2023, para. 64.

[233] McDonald, A. M., & Cranor, L. F. (2009). The Cost of Reading Privacy Policies. Journal of Law and Policy for the Information Society.

Regarding the availability of alternative services, DPAs appear to expect that data controllers provide an alternative option that is meaningful and fair while ensuring that the content and functionality remain identical or at least comparable across different versions of the service. Insights from empirical studies on pay-or-okay models further illustrate this issue: for instance, Müller-Tribbensee found that when faced with a pay-or-okay model, 99% of users opt for the tracking-based alternative.[234] Similarly, a web measurement study conducted by Morel[235] revealed that after contacting the CEO of the subscription management platform Contentpass for clarification on their pay-or-okay model, they were informed that 99.9% of visitors consent to tracking technologies. Additionally, Akman's survey, which included 11,151 respondents, indicated that only 9% of users would be willing to pay if Facebook introduced a €5 monthly fee for the same level of service.[236]

In addition, an industry-based survey demonstrated that only 3-10% of all users actively prefer to have their personal data processed for personalized advertising on Facebook.[237]

These empirical findings provide valuable insight into users' general unwillingness to pay and their perception of the fairness-or lack thereof-of alternatives within the pay-or-okay model. As for the characteristics of alternative services, their assessment remains largely subjective, as no clear criteria have yet been established to objectively determine whether two service offerings can be considered identical, and further empirical research is necessary to analyze user perceptions regarding what constitutes a fair or unfair alternative.[238]

Finally, DPAs require that consent be granular, meaning that users must have the ability to accept or decline consent for each specific purpose individually: this requirement suggests that a pay-or-okay consent banner should incorporate granular consent options at either the

[234] Müller-Tribbensee, T., Miller, K., & Skiera, B. (2024). Paying for Privacy: Pay-or-Tracking Walls, 5 March 2024.

[235] Morel, V., Santos, C., Fredholm, V., & Thunberg, A. (2023). Legitimate Interest is the New Consent – Large-Scale Measurement and Legal Compliance of IAB Europe TCF Paywalls. Proceedings of the 21st Workshop on Privacy in the Electronic Society. Copenhagen, Denmark.

[236] Akman, P. (2022). A Web of Paradoxes: Empirical Evidence on Online Platform Users and Implications for Competition and Regulation in Digital Markets. Virginia Law and Business Review.

[237] Van den Bergh, R. (2021). The German Facebook Saga: Abuse of Dominance or Abuse of Competition Law? World Competition.

[238] Davies, G. T. (2025). Consent or Pay: Transforming Internet Users from Products into Customers. Journal of European Consumer and Market Law.

first or second layer, as outlined in the EDPB's report on the work of the Cookie Banner Taskforce.[239]

Accordingly, Meta's model would need to introduce clear distinctions between different purposes and ensure that users can actively choose whether to accept or refuse consent for each specific data processing purpose - an option that is currently unavailable.[240]

Considering the policy-based recommendations from the EDPB and national authorities, Meta's pay-or-okay model can only be considered lawful if it meets the discussed requirements. If deemed legitimate, this model could extend beyond its current deployment on news websites and social networks, potentially being adopted by any industry sector capable of monetizing personal data through consent. This argument is supported by Morel, who demonstrates that such models are already prevalent across business, tech, and entertainment websites.[241]

The recommendations issued by DPAs, apart from certain regulatory decisions by the Austrian and German Lower Saxony DPAs, constitute soft law instruments and are therefore not binding on Meta. Consequently, in the DPA context, only rulings resulting from Austrian and Spanish DPA-based complaints could compel Meta to modify its current model.

Furthermore, most DPAs do not explicitly reference the freely given consent requirement but rather address it implicitly when discussing the necessity of an alternative service[242]; this omission likely stems from the assumption - shared by both the DPAs and the EDPB - that freely given consent is a fundamental prerequisite for legality under the GDPR.

Their detailed guidance, in turn, focuses on additional conditions that must be met for pay-or-okay models to be considered compliant. In other words, while the guidance presumes the presence of valid consent, it establishes further requirements to ensure the model's overall legality.

However, even if a model aligns with the conditions set out by DPAs, it would still be unlawful under the GDPR if it fails to meet the freely given consent requirement: as already

---

[239] EDPB, Report of the work undertaken by the Cookie Banner Taskforce. 17 January 2023 (adoption).

[240] Kerber, W., & Zolna, K. K. (2022). The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law. European Journal of Law and Economics, 34 pages.

[241] Müller-Tribbensee, T., Miller, K. M., & Skiera, B. (2024). Paying for Privacy: Pay-or-Tracking Walls.

[242] Only the Datenschutzkonferenz highlights the necessity of meeting all consent requirements (under Articles 4(11) and 7 GDPR) for a cookie paywall to be considered lawful.

mentioned, Meta's pay-or-okay model does not satisfy this requirement due to the inherent imbalance of power and the lack of unconditional choice, thereby failing to comply with the GDPR framework.

Moving to another legislative act, the DMA[243] is regarded as one of the key pillars of the European digital strategy, aiming to enhance the contestability and fairness of digital markets by imposing obligations on gatekeepers. Given the central role of data in digital markets, it is unsurprising that the DMA includes provisions regulating gatekeepers' data practices.[244]

Article 5(2) DMA seeks to limit gatekeepers' ability to accumulate data to foster a level playing field between them and other market participants: gatekeepers are prohibited from combining or cross-using personal data from their core platform services with data obtained from other services or third parties. However, this restriction applies only if users have not provided their consent. As such, Article 5(2) does not impose an outright ban on data processing but rather qualifies it, allowing gatekeepers to process data only if they obtain consent in accordance with the GDPR.[245] Under the DMA, consent is defined by reference to the GDPR, meaning that users must be given a specific choice and must be able to freely opt in to data processing.[121] This creates an overlap between the DMA and the GDPR, as the GDPR already governs the data processing activities covered by Article 5(2).

Since the GDPR came into force, the reliance on individual consent has faced repeated criticism. A key issue arises when individuals lack real choice in highly concentrated markets. In such cases, the imbalance of power between platforms and users may prevent consent from being freely given, as recognised in Meta. To address this challenge, the DMA introduces explicit safeguards to ensure that consent is genuinely voluntary. Specifically, the DMA requires gatekeepers to provide users with two options: one involving data processing under Article 5(2), which relies on consent, and another that excludes such processing (which may be offered for a fee).[246] The validity of consent for the first option depends on whether

---

[243] European Union. (2022). 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 (Digital Markets Act). Official Journal of the European Union, L 265/1.

[244] European Union. (2022). 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 (Digital Markets Act), Article 5. Official Journal of the European Union, L 265/1.

[245] GDPR, articles 4(11) and 8.

[246] De Streel, A., & Monti, G. (2024). Data-Related Obligations in the DMA. Centre on Regulation in Europe (CERRE), Implementing the DMA: Substantive and Procedural Principles, January 2024.

the second option, which does not require users to consent to data processing under Article 5(2), constitutes an "equivalent alternative".[247]

A key issue yet to be fully debated is the nature of the personalised and non-personalised versions of a service required to ensure valid consent. Two factors appear to be crucial.

First, the characteristics of an equivalent, non-personalised service must be clarified: the DMA states that "the less personalised alternative should not be different or of degraded quality compared to the service provided to the end users who provide consent, unless a degradation of quality is a direct consequence of the gatekeeper not being able to process such personal data".[248]

This implies that any reduction in quality must be demonstrably linked to the inability to process data otherwise restricted by Article 5(2) DMA and that any potential fee for the non-personalised service must be carefully assessed.

The DMA does not specify what level of fee would be considered legitimate. However, it is evident that the fee must be proportionate to the service offered to be deemed a realistic alternative to the personalised service. For example, doubts have been raised regarding the appropriateness of Meta's pricing for the non-personalised version of Facebook and Instagram, which costs €9.99 or €12.99 per month, depending on where it is purchased.

In March 2024, the European Commission launched a non-compliance investigation under the DMA, which includes an assessment of Meta's pay-or-okay model.[249] The investigation will examine whether Meta complies with Article 5(2), focusing on concerns that the binary choice presented to users may not constitute a genuine choice and may fail to prevent the accumulation of personal data.

According to the GDPR, as already mentioned, Meta's pay-or-okay model does not meet the standard for freely given consent, because consent is obtained in a manner that involves an unbalanced power dynamic, is conditional, lacks granularity, and is ultimately detrimental, which makes it incompatible with the requirements of Article 6 of the GDPR. While Data Protection Authorities (DPAs) have recognized that pay-or-okay models may be lawful, they

---

[247] European Union. (2022). 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 (Digital Markets Act), Recital 36. Official Journal of the European Union, L 265/1.

[248] Recital 37 of the DMA.

[249] European Commission. (2024). Press Release IP/24/1689 of 25 March 2024, Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act.

have imposed additional requirements, such as the need for a reasonable price and the availability of alternatives. However, these guidelines lack sufficient detail to effectively assess whether these conditions are met. As a result, even though Meta's model could potentially align with the DPAs' conditions after necessary adjustments, the user's consent cannot be considered as freely given under this model, which means it falls short of the GDPR's standards.

Under the Unfair Commercial Practices Directive[250], it becomes evident that this approach might qualify as an aggressive commercial practice, as it pressures consumers into making a choice. It could also be seen as misleading by creating the false impression that the presented choice is a result of recent legal changes.

From the perspective of Article 102 TFEU, while exploitative abuses have not always been the focus of enforcement, the European Commission has shown an increasing interest in addressing such practices in recent years.

Regarding the Digital Markets Act (DMA), the pay-or-okay model seems to fit the regulation's intent, though the specific requirements for its implementation remain vague. Nevertheless, since consent under the DMA refers back to the GDPR, any violation of the GDPR, such as invalidating freely given consent, would prevent gatekeepers from processing personal data in the ways outlined in Article 5(2) of the DMA.[251]

In conclusion, while the pay-or-okay model raises legal questions under the frameworks discussed, it is not necessarily illegal under consumer protection law, competition law, and the DMA. These frameworks allow for the resolution of issues, depending on the specificities of Meta's implementation.[252] Initially, this might also seem true under the GDPR, as DPAs have outlined conditions for a compliant cookie paywall model. However, it has been argued that Meta's model does not meet the requirement of freely given consent under the GDPR. Given the foundational importance of this requirement, it is argued that the analysis of the DPAs assumes that freely given (and informed) consent is a prerequisite for any pay-or-okay model to be lawful.[253] Therefore, it appears that Meta's model, in its current form, would be

[250] See note 178.

[251] Carugati, C. (2023). The 'pay-or-consent' challenge for platform regulators. Bruegel, Analysis 32/2023.

[252] Nettesheim, M. (2024). The Challenges of Regulating Pay-or-Consent Models. Verfassungsblog.

[253] Noronha, L. (2025). Meta's 'Consent-or-Pay' after the European Data Protection Board Opinion 08/2024: Is GDPR Compliance Possible? Tilburg Law School.

illegal under the GDPR. While the legal challenges under consumer protection law, competition law, and the DMA may be resolved, those arising from the GDPR's core condition of consent seem to be insurmountable.[254]

2.4.1 Meta Platforms Ireland v. EDPB: Meta's appeal against Opinion 08/2024 and its dismissal by the General Court

On June 27, 2024, Meta Platforms Ireland Ltd initiated legal proceedings[255] against the European Data Protection Board at the General Court of the European Union, challenging the EDPB's Opinion 08/2024, which evaluates the legitimacy of consent in *consent or pay* models used by large online platforms. Meta, in fact, as we are now well aware, at the end of 2023, revealed its intention to offer users in the European Union, European Economic Area, and Switzerland a paid subscription for ad-free access to Facebook and Instagram. The subscription was slated to launch in November 2023, priced at €9.99 per month for web access and €12.99 per month for iOS and Android devices.[256]

After the mention of the holding company of Facebook, Instagram and WhatsApp, in a footnote in the EDPB's Opinion[257], Meta filed for its annulment on June 27, 2024, and the action was published in the Official Journal of the European Union on August 12, 2024.[258] Meta's lawsuit outlines seven legal arguments challenging various aspects of the Opinion, addressing fundamental EU law issues, data protection, and the distribution of powers within the European Union. Meta's appeal, in fact, places significant emphasis on the respect for fundamental principles, referencing EU treaties and the Charter of Fundamental Rights more

[254] D'Amico, A. S., Pelekis, D., Santos, C., & Duivenvoorde, B. (2024). Meta's Pay-or-Okay Model: An Analysis Under EU Data Protection, Consumer, and Competition Law. Utrecht University School of Law Research.

[255] Max Schrems, founder of Noyb, criticized Meta's lawsuit against the EDPB, calling it "legal trolling" due to the unnecessary waste of time and financial resources it entails.

[256] Craddock, P. (2024). Op-Ed: A Critical Analysis of the EDPB's "Pay or Consent" Opinion.

[257] An EDPB Opinion is a non-binding instrument that the Board can issue in various contexts. It may provide guidance to the European Commission during the legislative process on data protection matters (under Article 70 GDPR) or, as in the case of the 'pay or consent' model, offer a consistency opinion when a national authority intends to adopt measures with cross-border implications (under Article 64 GDPR). Such opinions help ensure uniform application of data protection rules across the EU.

[258] European Union. (2024). Case T-319/24: Meta Platforms Ireland Ltd v European Data Protection Board, Action brought on 27 June 2024. Official Journal of the European Union, C/2024/4865. Available at: eur-lex.europa.eu.

than any other source, and arguing that the regulatory measures in question conflict with these foundational principles, particularly in terms of economic freedoms and the distribution of powers, which it believes are core tenets of the European legal system.

Meta's first plea questions the legality and applicability of Article 64(2) of the GDPR[259], asserting that the EDPB's interpretation violates fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union and disrupts the balance of powers within the EU. Precisely, Meta contends that EDPB Opinions cannot be directly challenged in court, which it views as a significant procedural limitation. Consequently, the company argues that Article 64(2) of the GDPR is either unlawful or, at a minimum, should be interpreted in a manner that prevents an excessive expansion of the EDPB's authority.

In its second plea, Meta claims the EDPB's opinion contradicts Article 19(1) of the Treaty on European Union[260] by misinterpreting the Court of Justice of the European Union's judgment in Case C-252/21, where the CJEU affirmed that Meta must allow users to opt out of targeted ads – "if necessary for an appropriate fee".

The third plea focuses on the disproportionate interference with Article 16 of the Charter, which guarantees freedom to conduct a business and Meta argues that the opinion does not adequately balance conflicting fundamental rights.[261]

Additionally, in its fourth plea, Meta contends that the opinion violates the principle of equal treatment enshrined in Article 20 of the Charter, suggesting that the opinion unfairly targets specific businesses or platforms.

The fifth plea is especially notable, as it accuses the EDPB of introducing a new, incoherent obligation not present in the GDPR, violating Article 52(1) of the Charter and undermining the principles of legal certainty, consent, and data minimization outlined in Articles 4(11) and

[259] Article 64(2) of the GDPR grants the European Data Protection Board (EDPB) the power to issue opinions when a supervisory authority, particularly in cases with cross-border implications, seeks guidance on a draft decision. This mechanism ensures consistency in GDPR enforcement across the EU. The requesting authority must take the EDPB's opinion into account, but it is not legally binding. If the authority does not follow the opinion, the matter may escalate to a binding decision under Article 65 GDPR.

[260] Article 19(1) of the Treaty on European Union (TEU) establishes the framework for the judicial system of the European Union. It mandates that Member States provide sufficient legal remedies to ensure effective judicial protection in fields covered by EU law. It also assigns the Court of Justice of the European Union (CJEU) the responsibility of ensuring the uniform interpretation and application of EU law. This provision reinforces the principle of the rule of law within the EU legal order.

[261] Notably, technology companies sometimes invoke this provision when they perceive that the actions of the European Data Protection Board (EDPB) could disproportionately affect their ability to operate within the EU legal framework.

5(1)(c) of the GDPR.[262] Meta effectively contends that the EDPB is engaging in arbitrary legal interpretation, formulating its positions without a solid legal basis. Moreover, Meta asserts that the EDPB's reading of the GDPR is so fundamentally flawed that it constitutes a breach of the rule of law.

Finally, the sixth and seventh pleas address procedural concerns: here, it's argued that the EDPB acted without impartiality, breaching Article 41(1) of the Charter, and claims its right to be heard under Article 41(2)(a) was disregarded during the opinion-making process; it is also asserted that the EDPB lacks impartiality and, while it is not the only company implementing a consent-or-pay model, the EDPB has announced its intention to issue a second, more broadly applicable opinion on the matter.[263]

On April 29, 2025, the EU General Court delivered an important decision in Case T-319/24, dismissing Meta's action against the European Data Protection Board's influential opinion on "consent or pay" models.[264]

In its order, the General Court clarified a key point that many had anticipated: opinions issued by the EDPB under Article 64(2) of the General Data Protection Regulation (GDPR) do not carry binding legal force and, critically, are not subject to annulment proceedings before the EU Courts: the Court rejected Meta's arguments, holding that the EDPB opinion does not produce binding legal effects and thus cannot be challenged under Article 263 of the Treaty on the Functioning of the European Union. According to the Court, the opinion serves merely as guidance, offering interpretative criteria to national supervisory authorities, which retain discretion in adopting their own decisions. As a result, no legal change arises for Meta until a competent authority adopts a specific measure based on that opinion.

Meta had also sought damages under Article 268 TFEU, arguing that the opinion would lead to decreased advertising revenue and loss of user subscriptions. This claim was likewise dismissed: the Court found the alleged harm to be hypothetical and noted the absence of a proven causal link, particularly given that no supervisory authority has yet required Meta to modify its business model.

---

[262] The principle of data minimization, as outlined in Article 5(1)(c) of the GDPR, requires that personal data be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Additionally, Article 4(11) defines consent as a freely given, specific, informed, and unambiguous indication of the data subject's wishes, which is particularly relevant in ensuring that only the necessary data are collected and processed.

[263] Bolognini, L., Covello, L., & Fiordalisi, G. (2024). Admissibility of the "Pay or Consent" Model.

[264] The decision is available at the following link: General Court vs. Meta .

It is likely that this decision will be appealed by Meta before the Court of Justice, particularly in light of the fact that, with well-reasoned arguments, an Advocate General[265] has recently suggested that a broader range of acts may be challengeable than the General Court recognized in the Order under discussion.[266]

In this regard, the AG has clarified that certain factors are irrelevant when assessing whether an act of an EU institution may be challenged before the General Court: importantly, she observed that it is immaterial whether an act is an "intermediary act" (such as an EDPB Binding Decision that precedes the adoption of a decision by the competent supervisory authority). The decisive criterion is whether the act constitutes a "final and binding act" on its own merits. According to the AG, a Binding Decision represents the EDPB's definitive position and imposes an obligation on a party external to the Board - in this instance, the Irish Data Protection Commission.[267] The AG further emphasized that all acts of EU institutions and bodies, irrespective of their form or designation, are considered challengeable if they are intended to produce binding legal effects.[268]

A crucial distinction was drawn between the requirements for establishing whether an act is challengeable and the separate inquiry into whether it directly concerns the applicant. Specifically, whether an act brings about a "distinct change" in the legal position of the applicant is a question relevant to the assessment of "direct concern", not to the determination of challengeability.[269] With regard to the requirement of "direct concern", two cumulative conditions must be met in order for an applicant to bring a challenge against a challengeable act: first, the contested measure must have a direct impact on the applicant's legal situation; second, it must leave no discretion to the authorities responsible for its implementation, such that implementation is automatic and derives solely from EU law, without the need for further intermediate rules or measures.[270]

---

[265] Ms. Tamara Ćapeta.

[266] Reference is made to Opinion of Advocate General Ćapeta delivered on 27 March 2025, Case C-97/23 P, WhatsApp Ireland Ltd v European Data Protection Board.

[267] AG Ćapeta Opinion, Case C-97/23 P, paras. 42, 44, 70, and 82.

[268] AG Ćapeta Opinion, Case C-97/23 P, para. 74.

[269] AG Ćapeta Opinion, Case C-97/23 P, para. 83.

[270] AG Ćapeta Opinion, Case C-97/23 P, para. 128.

2.4.2 BEUC's latest evaluation of Meta's Pay-or-Consent Policy for online users

Meta's latest pay-or-consent model for Facebook and Instagram[271], implemented in November 2024, has also been scrutinized in January 2025 by the European Consumer Organisation (BEUC)[272] for its potential violations of European Union laws, including the Unfair Commercial Practices Directive[273], the General Data Protection Regulation, and the Digital Markets Act. Meta's subscription model presents users with two primary choices: they can either consent to extensive data collection and personalized advertising or pay a subscription fee to access an ad-free version of the service. After opting into data processing, users are given an additional choice between fully personalized ads and "less personalized" ads. BEUC contends that this model continues to violate European laws by misleading consumers, failing to ensure valid consent, and imposing unfair conditions on users.[274]

One of the primary concerns raised by BEUC is the deceptive nature of Meta's pay-or-consent model in light of EU consumer protection laws: the organization argues that Meta's messaging surrounding the model creates confusion among users, particularly through ambiguous wording. For instance, Meta's description of the free version as "use free of charge with ads" implies a zero-cost service, even though consumers are effectively paying with their personal data. This phrasing is particularly problematic in languages where "free" has a more explicit connotation of a cost-free service, misleading users into underestimating the true cost of their choice.[275]

Additionally, BEUC highlights that Meta's interface design employs "dark patterns"[276] that nudge users towards consenting to data collection rather than opting for the paid version.

---

[271] Meta. (2024). Facebook and Instagram to Offer Subscription for No Ads in Europe (12 November 2024). Available at: https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/.

[272] The European Consumer Organisation (BEUC) is an umbrella group representing consumer organizations from across Europe. It advocates for consumer rights and interests in EU policymaking, covering areas such as digital rights, competition, and product safety.

[273] See note 178.

[274] Baltag, A., & Leszczynska, A. (2024). "Can I have it non-personalised?" An Empirical Investigation of Consumer Willingness to Share Data for Personalised Services and Ads. Journal of Consumer Policy.

[275] Arthur Cox LLP. (2024). Critical Analysis of EDPB Opinion 08/2024.

[276] For a definition of "dark patterns", see note 108.

These interface elements, such as the pre-selection of options and the use of prominent visual cues, obscure the true implications of the user's choices. Such manipulative design techniques undermine the principle of informed decision-making, which is a cornerstone of EU consumer protection law.

In terms of GDPR compliance[277], BEUC raises several concerns regarding Meta's approach to user consent. The organization argues that the consent required for personalized advertising does not meet the GDPR's standard of being freely given, specific, informed, and unambiguous: one key issue is that users are forced to choose between consenting to extensive data processing or paying a fee, creating a coercive environment that limits genuine choice. This form of consent bundling contradicts the European Data Protection Board's binding decisions, which emphasize that consent must not be tied to the provision of a service.

Furthermore, the *pay-or-consent* model does not allow users to provide separate consent for different types of data processing: for instance, Meta collects data from users' on-platform activity, such as content interactions, as well as off-platform activity, such as browsing behavior tracked through Meta's advertising tools. GDPR requires that users be given the ability to provide granular consent, meaning they should be able to opt into one type of data processing while refusing another. By failing to offer such an option, Meta's model does not align with GDPR requirements.

BEUC also points out that the process of withdrawing consent is made difficult, further undermining the validity of the initial consent[278], and arguing that users who attempt to withdraw consent from Meta's data processing face barriers that discourage them from doing so. This includes the potential degradation of their user experience, as those who choose "less personalized ads" face more frequent ad interruptions. According to the EDPB, if users experience detriment when withdrawing consent, it indicates that their consent was never valid in the first place.[279]

---

[277] Ensuring compliance with key aspects of the GDPR is vital for meeting the requirements of the Unfair Commercial Practices Directive and the Digital Markets Act, and the reverse is also true. The application of GDPR principles, such as transparency and consumer rights, influences how businesses manage commercial conduct and digital market operations, promoting alignment between these legal frameworks to safeguard consumers and maintain fair competition in the digital environment.

[278] The GDPR, in fact, states that withdrawing consent should be as easy as giving it.

[279] For further details on how, according to BEUC, Meta is breaching consumers' fundamental rights, refer to the document available at the following link: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2024-020_How_Meta_is_breaching_consumers_fundamental_rights.pdf.

Another critical issue pertains to the principle of data minimization, which requires companies to limit data collection to what is strictly necessary for the stated purpose: BEUC argues that Meta continues to collect excessive amounts of data, even for users who opt for the "less personalized ads" option, and it highlights that Meta does not provide clear information on what data is processed under this model, leaving users in the dark about the extent of data collection. Additionally, the company does not set clear retention periods for the data it collects, meaning that personal information may be stored indefinitely, further violating GDPR principles.

Beyond consumer and data protection laws, Meta's pay-or-consent model is also scrutinized under the Digital Markets Act, which establishes obligations for designated gatekeepers like Meta. Under Article 5(2) of the DMA, gatekeepers must obtain valid consent before processing personal data for targeted advertising. BEUC argues that Meta's approach does not meet this standard because it employs manipulative tactics to steer users toward consenting to data collection.

The DMA also requires that companies provide users with a non-degraded alternative if they choose not to share their data. However, BEUC contends that the introduction of unavoidable ad breaks in the "less personalized ads" model constitutes a deliberate degradation of service, designed to push users towards consenting to data collection.

Finally, BEUC raises concerns about Meta's processing of third-party data: under the DMA, gatekeepers must obtain explicit consent before using personal data collected from third-party sources, such as external websites and applications. Meta's policies, however, suggest that it continues to aggregate data from multiple sources without clear and explicit user consent. This raises compliance concerns under both the DMA and GDPR, as users are not given adequate control over how their data is used across different platforms.

To address these concerns, BEUC calls for coordinated enforcement actions by various EU regulatory bodies. It urges the Irish Data Protection Commission (Meta's lead data protection authority in the EU) and the European Data Protection Board (EDPB) to investigate Meta's GDPR compliance and take corrective measures. The organization also calls on the European Commission and the Consumer Protection Cooperation (CPC) Network to take action under consumer protection laws[280], particularly regarding Meta's misleading

[280] The BEUC members participating in this action are: Consumentenbond (Netherlands), dTest (Czech Republic), Vartotojų aljansas (Lithuania), Adiconsum (Italy), EKPIZO & KEPKA (Greece), UFC-Que Choisir (France), Asufin & CECU (Spain), Spoločnosť ochrany spotrebiteľov (S.O.S.) Poprad (Slovakia), ZPS (Slovenia), Forbrugerrådet Tænk (Denmark), Latvijas Patērētāju interešu aizstāvības asociācija (Latvia),

advertising practices, also advocating for stronger enforcement of the DMA to ensure that Meta adheres to its obligations as a designated gatekeeper.

In conclusion, BEUC's analysis of Meta's pay-or-consent model highlights significant legal and ethical concerns. The model is – once again – suspected of violating multiple EU laws by misleading consumers, failing to ensure valid consent, and creating an unfair digital marketplace. BEUC's call for regulatory intervention underscores the need for stronger enforcement mechanisms to protect consumer rights and ensure that large tech companies comply with EU legal standards.[281]

2.5 Case C-21/23

Even more recently, the Court of Justice of the European Union has ruled on the role of consent under the GDPR, but in a different market context. Case C-21/23[282] represents a natural extension of the reasoning established in the Facebook v. Germany case (Case C-252/21), as both rulings scrutinize the conditions under which consent to data processing can be considered freely given. While the Facebook Germany case dealt with the intersection of competition law and data protection in the context of a dominant online platform, *Lindenapotheke* extends this discussion into the pharmaceutical e-commerce sector. The common thread between these cases is the requirement that consent be explicit, informed, and freely given, reinforcing the GDPR's emphasis on user autonomy and data protection as a fundamental right.

In Facebook Germany, the CJEU ruled that a dominant online platform could not impose behavioral advertising as a precondition for access to its social networking services, emphasizing that users must be able to make a genuine choice regarding their data, and establishing that the mere acceptance of terms and conditions does not automatically constitute valid consent under the GDPR if users lack an alternative to using the service without agreeing to extensive data collection.

Federacja Konsumentów & Fundacja Konsumentów (Poland), Sveriges Konsumenter (Sweden), Union Luxembourgeoise des Consommateurs (Luxembourg), Forbrukerrådet (Norway), Асоциация Активни потребители (Bulgaria).

[281] BEUC. (2025). Assessment of Meta's Latest Pay-or-Consent Policy for Facebook and Instagram Users, January 2025.

[282] Case C-21/23, Lindenapotheke, preliminary ruling request dates back to 19 January 2023.

Similarly, in *Lindenapotheke*, the CJEU reaffirmed the stringent requirements for valid consent but in a different market context: the case concerned a dispute between two competing pharmacists in Germany. One of them, *Lindenapotheke*, sold pharmacy-restricted medicines via Amazon without obtaining explicit consent from customers for processing their health-related data. A competing pharmacist challenged this practice under national unfair competition laws, arguing that the failure to secure explicit consent for processing health data violated GDPR provisions, thereby constituting an unfair commercial practice.[283]

The CJEU held that health-related data collected during online medicine purchases fell within the GDPR's special category of sensitive data under Article 9.[284] Consequently, explicit consent was required before processing such information. The ruling clarified that even when a product is not prescription-based, the data collected in the transaction (such as a customer's choice of medicine) could reveal health-related information, necessitating the highest level of protection under the GDPR. The decision further emphasized that national legislation allowing competitors to challenge GDPR violations under unfair competition laws was compatible with EU law, as such mechanisms reinforced the GDPR's objectives of ensuring high levels of data protection.

Therefore, *Lindenapotheke* case builds upon Facebook v. Germany in at least three key aspects. First, it underscores that valid consent must be obtained in a manner that truly reflects user choice, regardless of whether the data processing occurs in the digital advertising sector or pharmaceutical transactions. In both cases, the CJEU scrutinized whether consent was freely given and whether users had sufficient control over their data. Facebook Germany highlighted the risk of coercion when users of a dominant platform have no real alternative, while *Lindenapotheke* addressed similar concerns in a consumer healthcare setting, where individuals may not be fully aware of the extent to which their personal information is being processed.

Secondly, both cases reinforce the principle that contractual necessity cannot serve as a blanket justification for extensive data processing. In Facebook v. Germany, Meta's argument that targeted advertising was necessary for the performance of its contractual obligations was rejected. Similarly, in *Lindenapotheke*, the court made it clear that a pharmacy's online sales model could not bypass the requirement for explicit consent simply because

[283] Press Release No. 159/24, Court of Justice of the European Union, Case C-21/23, Lindenapotheke, 4 October 2024.

[284] Ibid.

collecting customer data was an inherent part of the transaction. The necessity test under GDPR remains stringent, requiring companies to demonstrate that data processing is indispensable for service delivery rather than merely useful or commercially beneficial.[285]

The rulings collectively illustrate an evolving judicial stance on GDPR enforcement mechanisms: Facebook v. Germany established that data protection violations could be examined in the context of competition law, allowing antitrust authorities to assess abusive practices that involved the misuse of personal data, while *Lindenapotheke* extended this enforcement scope by confirming that GDPR violations could also be challenged under unfair competition laws by private competitors. This expansion of enforcement avenues strengthens data subjects' rights by ensuring that multiple stakeholders-competition authorities, national regulators, and private actors-can hold businesses accountable for non-compliance with data protection rules.[286]

Beyond their legal implications, these cases highlight the broader economic and policy debates surrounding data protection, market fairness, and consumer choice in digital and healthcare environments.[287] The Facebook v. Germany ruling directly influenced how companies structure their business models in response to GDPR restrictions, leading to the rise of alternative approaches such as subscription-based access to digital services without targeted ads. *Lindenapotheke*, in turn, has profound implications for the online sale of pharmaceutical products, potentially requiring businesses to redesign their consent mechanisms to meet the explicit consent standards for sensitive data processing.

In conclusion, both these cases collectively contribute to a coherent jurisprudential approach to GDPR enforcement, emphasizing that consent must be freely given, specific, and informed, regardless of the industry in question. The CJEU's rulings reaffirm that data subjects' rights cannot be circumvented through contractual terms, dominant market positions, or business models that rely on extensive data collection. By extending the principles established in Facebook Germany to the healthcare sector, *Lindenapotheke* further cements the idea that GDPR compliance is a fundamental obligation across all industries where personal data processing occurs. As digital services and e-commerce continue to evolve, these rulings provide a legal framework that prioritizes user autonomy and data

[285] European Law Blog, Case C-21/23 Lindenapotheke – Competitors can enforce GDPR-based unfair commercial practices.

[286] Taylor Wessing, "Judgment of the ECJ in case C-21/23 (Lindenapotheke)," October 2024.

[287] Ibid.

protection, setting the stage for future regulatory developments in both digital and offline markets.

We therefore understand that data protection is no longer merely a matter of compliance; it is evolving into a strategic asset that can provide a competitive advantage. In an era where digital trust is a key differentiator, companies that embrace data protection as a core business value position themselves ahead of competitors, enhancing their reputation and long-term sustainability.

2.6 *Actio finium regundorum* between the Italian Competition Authority (AGCM) and the Italian Data Protection Authority on unfair commercial practices: the Council of State's ruling on the appeal against Judgment No. 15326 of November 2022

In a recent ruling issued by the Council of State in a case involving Google Ireland Ltd. and the Italian Competition Authority (AGCM), an in-depth examination has been conducted on the complex issue of the division of competences between the Antitrust Authority and the Data Protection Authority in matters concerning unfair commercial practices.

With Judgment No. 80 of January 7, 2025[288], the Council of State ruled on the appeal filed against Judgment No. 15326 of November 18, 2022[289], issued by the Regional Administrative Court[290] for Lazio. The latter had rejected the challenge against the decision adopted by the Italian Competition Authority (AGCM) on November 16, 2021, concerning two distinct practices carried out by Google Ireland Ltd. These practices involved the collection and use of user-consumer data for commercial purposes, both during the creation of a Google ID and when accessing other services offered by the company, which also entailed data collection. For each of these practices, the AGCM imposed an administrative fine of €5,000,000, identifying two distinct unfair commercial practices.

The first practice concerned the information provided by Google during the creation of a user account-an essential step for accessing all the services offered by the company-as well

[288] Available, for subscribers, at this link: Fair Play - Full Text.

[289] Available, for subscribers, at this link: Fair Play - Full Text.

[290] The Regional Administrative Court is also referred to as TAR (Tribunale Amministrativo Regionale).

as during the use of various Google services: the information presented to users was found to lack immediacy, clarity, and completeness regarding the collection of personal and search data for commercial purposes.

The second practice involved the mechanism through which Google obtained user consent for data processing with commercial purposes: the company employed an opt-out system, meaning that users were not given a prior and explicit choice regarding the collection and use of their data. Instead, the default setting permitted data collection during the creation of a Google ID, a necessary step for accessing most of Google's services.

In an initial and structured set of arguments, Google challenged the jurisdiction of the Antitrust Authority on two distinct grounds: the overarching and exclusive competence of the Data Protection Authority and the absence of a consumer relationship.

Regarding the interplay between regulations on unfair commercial practices and data protection rules, Google argued that the latter should take precedence over the former. Furthermore, it contended that the activities addressed in the contested decision did not constitute a commercial decision, as they did not represent the price or consideration paid by users to access the services offered.

The Council of State recalled that administrative case law, including references to European jurisprudence, had already examined the relationship between the Antitrust Authority and sectoral regulators in this area, reaching conclusions that the court fully endorsed.

Both European and national case law have established that the principle of specialty, which would grant exclusive jurisdiction to the sectoral authority, should be subordinated to the principle of incompatibility. According to this approach, the sectoral authority may intervene only when the contested conduct falls within a specific domain that does not overlap with the Antitrust Authority's scope of action.

In other words, incompatibility - and thus the jurisdiction of the sectoral authority - exists only when the conduct in question can exclusively be addressed by that authority. Conversely, if the contested conduct falls, even in abstract terms, within the jurisdiction of both authorities, competence is attributed to the Antitrust Authority rather than the sectoral regulator.

The most recent administrative jurisprudence, including the judgments of the Council of State No. 6077 of July 9, 2024, No. 5030 of June 5, 2024, and No. 3175 of April 5, 2024, has reaffirmed a well-established approach regarding the allocation of competence between the Competition Authority and sector-specific regulatory bodies. According to this approach,

European law, particularly Article 3(4) of the Unfair Commercial Practices Directive[291], establishes that, in cases of conflict between the provisions of the Directive and other EU rules governing specific aspects of unfair commercial practices, the latter shall prevail. However, European case law has clarified that this provision applies solely to conflicts between EU norms and does not extend to relationships between EU and national legislation. Moreover, the scope of this principle is significantly limited, applying only in circumstances where external provisions impose obligations on professionals that are inherently incompatible with those established by the Directive on unfair commercial practices. Outside of this scenario, national legislation may legitimately assign the competence to sanction such practices to the Competition Authority rather than the relevant sector-specific authority.

In this regard, the Court of Justice of the European Union, in its judgment of September 13, 2018 (Case C-54/17), has emphasized that the notion of "conflict" between consumer protection legislation and sectoral regulations should not be resolved through the principle of specialty but rather through the criterion of incompatibility. This criterion dictates that a conflict arises only when the divergence between the two regulatory frameworks is so fundamental that it precludes their coexistence. Consequently, for an actual conflict to be recognized, sector-specific provisions must impose obligations that are irreconcilable with those set out in Directive 2005/29/EC on unfair commercial practices.

As a result, the appropriate standard for determining the allocation of competence between the Competition Authority and sector-specific regulators is not the principle of specialty but that of incompatibility. This perspective, which has also been upheld in the jurisprudence of the Council of State (Section VI, Judgments No. 665 of 2021 and Nos. 7296 and 4357 of 2019), implies that, as a general rule, the authority responsible for sanctioning unfair commercial practices is the Competition Authority, while sectoral regulators may intervene only when their respective frameworks regulate specific aspects in a manner that renders them incompatible with general unfair commercial practices legislation.

Accordingly, the relationship between the Consumer Code and sectoral regulations should be understood as one of complementarity and harmonization rather than mutual exclusion. The assessment of incompatibility between the two legal frameworks must be conducted on

[291] See note 178.

a case-by-case basis, ensuring that both sets of rules can coexist without requiring the elimination or subordination of one to the other.

According to the Council of State, the legal principles referenced are applicable to the case at hand, even though the appellant rightly argued that privacy regulations are general rules, applicable across all sectors. This consideration pertains to the correctness of personal data processing, which affects all areas of social life horizontally, with the aim of safeguarding the associated personal rights. However, it does not concern the transparency of information regarding the commercial exploitation of such data within a consumer relationship.

In other words, privacy legislation is intended to protect personal rights, not to safeguard consumer freedom. Therefore, in this context, privacy law constitutes sector-specific legislation, just like other regulatory frameworks, which leads to the application of the principles outlined. In this regard, the Council of State[292] clarified that the issue at hand was not about determining whether consumer law could overlap with data protection law, as these two "rights" belong to distinct sectors and are governed by specific regulations that should not overlap; instead, the ruling emphasized that what was at issue in the case was the exploitation of personal data by the two companies, which the user had unknowingly provided at the time of registration. The Court acknowledged that the notion of "processing" personal data, as defined in Article 4, paragraph 2, of the GDPR, encompasses a wide range of uses of personal data and that the special data protection rules of the European Union extend to a very broad array of human or automated relations involving personal data. However, it stressed that it would be unreasonable to interpret the scope of the exclusive and special nature of the GDPR as an "absolute" framework that would exclude the applicability of other legal norms. Such a conclusion would be deemed irrational, as all areas of law and human conduct, including those involving automatic mechanisms related to digital tools, inherently involve personal data. Thus, recognizing the absolute specificity of data protection law would lead to the exclusion of other legal frameworks, which is not feasible. While the centrality of the GDPR and national privacy laws in protecting personal data is acknowledged, the Court argued that when the processing of personal data intersects with behavior and situations governed by other legal sources that protect equally important values and interests, such as consumer protection, the legal system must ensure that these sector-

[292] Council of State. Judgment of March 29, 2021, No. 2631.

specific laws are applicable. This would prevent a reduction in the protections afforded to individuals under other relevant legal frameworks.

The conduct addressed in the decision adopted by the Italian Competition Authority in relation to Google falls within the scope of a consumer relationship and, therefore, constitutes commercial decisions. According to Article 3 of Legislative Decree No. 206 of 2005, a consumer or user is defined as a natural person acting for purposes unrelated to entrepreneurial, commercial, artisanal, or professional activities. On the other hand, a professional is defined as a natural or legal person acting in the exercise of their entrepreneurial, commercial, artisanal, or professional activities, or their intermediary. A product is any product intended for the consumer, even as part of a service, provided or made available for a fee or free of charge within a commercial activity.

The subject of the investigation conducted by the Antitrust Authority pertains not to the fairness of personal data processing, which falls under the jurisdiction of the Data Protection Authority, but to the manner in which information is provided regarding the commercial use of such data in the context of a consumer relationship. In other words, the Authority contested not the violation of a personality right related to personal data processing, but rather the opacity and inadequacy of information regarding the use of personal data for commercial purposes.

This use relates to a consumer relationship involving the so-called "monetization of personal data", typical of the new economies within digital markets. The exploitation of personal data is framed as a counter performance for the service offered by the professional, as it holds commercial value. The professional collects personal data from users and uses it for profiling purposes for third parties, selling advertising space and engaging in other advertising intermediary activities.

In essence, a triangular relationship is created: the consumer accesses Google's services, unwittingly allowing, though not necessarily required (the critical issue raised by the Antitrust Authority being the lack of correct and adequate information), the use of their personal data by Google, which in turn shares the data with third parties in exchange for compensation for advertisements.

In other words, consumers access Google's services while Google sells the profiled personal data in exchange for payment, and businesses pay for the advertising of their products.

The revenues derived from advertising services, resulting from profiling activities, constitute the primary source of income for Google. Furthermore, the appellant argued that it is well

known that all online services need to cover their costs, and that, with the exception of Wikipedia and institutional websites, all online services not behind a paywall are monetized through advertising.

The primary aim of profiling is to collect personal data and transform it into information used to create advertisements and sponsorships tailored to the user's interests, with the goal of driving the purchase of specific products or services. It is irrelevant that Google could provide services to users even without using their data, as the lack of transparency is intentionally designed to exploit personal data for commercial purposes. The economic value of such data becomes apparent, albeit indirectly, as it serves as a *commodity* for businesses that, in exchange for payment, deliver personalized advertising to individual users. Profiling cookies are used to build user profiles and are employed to send advertisements that align with the preferences demonstrated by the user during online browsing.

Regarding the division of competence between the Antitrust Authority and the Data Protection Authority, the appellant raised several preliminary issues, requesting that the case be referred to the Court of Justice of the European Union under Article 267, paragraph 3, TFEU[293], both in the appeal and in the final memorandum. However, the Council of State considers itself exempt from the obligation to refer the case, as the interpretation of Union law in this case, considering existing European jurisprudence, is so clear that there is no reasonable doubt. It has been pointed out that the European Court established the so-called incompatibility criterion, rather than the specialty criterion, to determine the competent authority in matters of unfair commercial practices.

In this context, it must be emphasized that while privacy regulations are transversal, applying across various sectors, they aim to protect personal rights rather than the freedom of the consumer. Therefore, in the realm of unfair commercial practices, privacy regulations should be viewed as a sectoral law, similar to others, and the incompatibility criterion set by European jurisprudence applies. In other words, while privacy laws, in relation to personal data protection, have a *horizontal* nature, applying across all areas of social activity, when data is used for commercial purposes, such regulations take on a *vertical* nature and are not incompatible with specific sectoral regulations.

[293] Article 267(3) TFEU establishes the obligation for courts of last instance to refer a question to the Court of Justice of the European Union (CJEU) when a case raises a question on the interpretation or validity of EU law, ensuring uniform application across Member States.

As rightly pointed out in paragraph 50 of the contested decision, in order to protect one of the fundamental human rights, the Data Protection Authority has the competence to impose sanctions for violations of the obligations set forth in privacy law. Meanwhile, the Consumer Code, in the context of unfair commercial practices, is tasked with protecting the consumer from economic decisions induced by misleading or aggressive practices. Therefore, the right to privacy and the Consumer Code have distinct fields of application and pursue different interests, while complementing each other.

In the case at hand, no provision of privacy law specifically addresses aspects of unfair commercial practices, imposing obligations on professionals that are incompatible with those established by Directive 2005/29. Hence, based on the regulatory framework clarified by the Court of Justice of the European Union, the Antitrust Authority must be considered unquestionably competent to adopt the contested decision.

Regarding Google's claims about the validity of the two unfair commercial practices under scrutiny, and specifically the aggressive nature of the practices in question, the Council of State considers Google's objections unfounded with respect to the first unfair practice, but deems the objections valid concerning the second practice.

Legislative Decree No. 206 of 2005[294] defines an aggressive commercial practice as one that, in a given situation and considering all relevant characteristics and circumstances, limits or has the potential to significantly restrict the consumer's freedom of choice or behavior through harassment, coercion-including the use of physical force-or undue influence. Consequently, such a practice leads or is capable of leading the consumer to make a commercial decision that they would not have otherwise made.

Similarly,[295] the Code outlines the criteria for determining whether a commercial practice involves harassment, coercion (including the use of physical force), or undue influence. The assessment takes into account various factors such as: the timing, location, nature, or persistence of the practice; the use of physical or verbal threats, or the exploitation by the professional of any tragic event or specific circumstances.

In this case, the Authority determined the existence of undue influence capable of significantly restricting the average consumer's freedom of choice.

[294] Art. 24, "Aggressive Commercial Practices".

[295] Art. 25, "Use of Harassment, Coercion, or Undue Influence".

The objections raised appear to be well-founded, particularly in light of Google's argument that the contested decision failed to take into account that Google had, in fact, asked users multiple times whether they wished to receive personalized ads. This was done through pop-ups displayed both at the beginning and at the end of the registration process.

In other words, the preselection of available options does not result in an immediate and direct transmission of data. Moreover, additional steps follow, allowing consumers to deselect the setting that enables data profiling for commercial purposes. In this regard, reference is made to the rulings of the Council of State, Section VI, of December 2, 2024, No. 9614, and March 29, 2021, No. 2631.

It must also be considered that the pre-setting of consent for data transfer to receive personalized ads does not, in itself, constitute an aggressive commercial practice.

For a commercial practice to be classified as aggressive, there must be an additional element (*quid pluris*) that translates into conduct capable of coercing the user's freedom of choice-something that does not appear to be present in this case. The use of an opt-out rather than an opt-in mechanism, in the absence of other aggravating factors, may contribute to a misleading commercial practice but does not amount to the undue influence required under Article 24 of the Consumer Code. This is because, even if through a more cumbersome process, the consumer can still avoid making the proposed choice by deselecting the default option and selecting a different one.

Ultimately, the lack of information about the effects of pre-selection is relevant in terms of misleading consumers and affecting their awareness but not in terms of aggressiveness-that is, their freedom of choice. The system employed by the company, therefore, may reasonably be deemed capable of misleading the average consumer but not of restricting their ability to choose freely.

In any case, the two contested commercial practices do not exhibit structural and functional autonomy, as they both concern the methods of obtaining consumer consent for the same products, occur within the same temporal and procedural framework, and serve the identical purpose of processing personal data for commercial purposes.

From a teleological-functional perspective, Google's conduct can thus be considered as a single practice, given that both contested actions were aimed at obtaining consent for the delivery of standardized advertising messages. As a result, the imposition of cumulative penalties was unjustified.

Consequently, based on these considerations, the Council of State has ruled that Google's appeal should be partially upheld concerning the second contested commercial practice, whereas it should be rejected in all other respects regarding the first.

2.7 Integrating market and competition factors into data protection practices: the EDPB's position paper (January 2025)

As examined in the preceding pages, the evolving interplay between data protection and competition law necessitates a reassessment of regulatory approaches to ensure coherence and effectiveness in enforcement. As underscored by the EDPB[296], while these two legal frameworks pursue distinct objectives, they exhibit significant intersections, particularly in the context of digital markets where the collection, processing, and use of personal data have become central elements of business models. The primary purpose of data protection law is to safeguard individuals from unlawful and opaque processing of personal information, ensuring the respect of fundamental rights, whereas competition law seeks to maintain the integrity of markets, preventing anti-competitive conduct that could lead to consumer harm. However, in an increasingly data-driven economy, the boundaries between these two disciplines are progressively blurred, creating a need for enhanced regulatory collaboration and mutual recognition of overlapping concerns.

A key aspect of this interplay is the recognition that data can serve as both a market asset and a parameter of competition.

The European Commission has acknowledged that in defining relevant markets, privacy and data protection considerations may constitute competitive differentiators, particularly in digital and technology-driven sectors. This development signals a shift in regulatory perspectives, whereby access to and control over personal data may confer a competitive advantage that warrants scrutiny under competition law. The CJEU's judgment in Case C-252/21 further reinforces this notion by confirming that competition authorities, when assessing potential abuses of dominance, cannot disregard the implications of data processing under the GDPR. The ruling explicitly establishes that while competition regulators must respect the primary jurisdiction of data protection authorities, they nonetheless have a duty

[296] European Data Protection Board. (2025). EDPB Position Paper on Interplay between Data Protection and Competition Law. Adopted on 16 January 2025.

to consider data protection principles when evaluating market power and business practices that may distort competition.

Moreover, the necessity of fostering structured cooperation between regulatory bodies has become evident, particularly in light of the disparities in existing national frameworks governing the interaction between data protection and competition authorities. Currently, the degree of cooperation varies significantly across Member States, ranging from ad hoc consultations to formalized agreements and legally mandated collaborative mechanisms. The EDPB has emphasized the need for a harmonized approach that promotes the systematic exchange of expertise, coordination in enforcement actions, and joint initiatives where appropriate. Enhanced cooperation is particularly crucial in cases involving large digital platforms, where data-driven market dominance raises complex concerns spanning both legal regimes. The experience with enforcement actions against major technology firms demonstrates that an isolated application of either data protection or competition law may be insufficient to address the full spectrum of regulatory challenges posed by dominant digital actors.

A notable illustration of this evolving dynamic is the increasing scrutiny of mergers and acquisitions in the digital economy from a data protection standpoint. The EDPB has pointed to the potential risks associated with corporate consolidations that lead to extensive aggregation of personal data, thereby reinforcing market dominance and reducing consumer choice. In this regard, privacy considerations are not merely ancillary to competition assessments but constitute integral elements that can influence market structures and competitive dynamics. The Digital Markets Act further underscores the importance of curbing exploitative data practices by imposing obligations on designated gatekeepers[297], ensuring that dominant firms do not leverage personal data in a manner that undermines market fairness and contestability.

To enhance regulatory coherence, the EDPB suggests several practical measures aimed at strengthening collaboration between data protection and competition authorities. These include the establishment of dedicated teams within regulatory agencies to facilitate inter-agency coordination, the development of joint investigation protocols, and the creation of shared analytical frameworks that integrate both data protection and competition considerations. Additionally, mechanisms such as joint workshops, expert working groups,

[297] See note 141.

and structured information-sharing agreements could serve to bridge existing gaps and foster a more integrated regulatory approach. The principle of sincere cooperation, as enshrined in Article 4(3) TEU, provides a legal foundation for such collaborative efforts, mandating that EU institutions and national authorities work together in a mutually supportive manner to ensure the effective implementation of Union law.

In conclusion, the increasing convergence of data protection and competition law necessitates a recalibration of regulatory strategies to address the multifaceted challenges posed by data-driven business models. The EDPB's position underscores the imperative of fostering synergies between these legal frameworks, ensuring that enforcement actions reflect a holistic understanding of both consumer protection and market integrity: by advancing cooperative mechanisms and integrating data protection considerations into competition assessments, regulators can more effectively safeguard individual rights while promoting a competitive and innovative digital economy. The path forward requires a concerted effort to harmonize regulatory interpretations, enhance cross-sectoral dialogue, and develop forward-looking policies that account for the evolving digital landscape. Through sustained cooperation and the adoption of best practices, data protection and competition authorities can jointly contribute to a more coherent and effective regulatory ecosystem that upholds both fundamental rights and market fairness.

CHAPTER 3.

Latest developments and future directions

Summary: **3.1** The approach of European Data Protection Authorities to the "consent or pay" model - **3.1.1** The ICO's approach - **3.1.2** The Norwegian Data Protection Authority's approach - **3.1.3** The Dutch Data Protection Authority's approach - **3.1.4** The Belgian Data Protection Authority's approach - **3.1.5** The Spanish Data Protection Authority's approach - **3.1.6** The Austrian Data Protection Authority's approach - **3.1.7** The French Data Protection Authority's approach - **3.1.8** The German Data Protection Authority of Lower Saxony's approach - **3.1.9** The Italian Data Protection Authority's approach - **3.2** Meta found in breach of the Digital Markets Act: European Commission's April 2025 Decision - **3.3** An alternative third option beyond the "consent or pay" model - **3.4** Balancing data protection and market efficiency: towards a coherent regulatory approach - **3.5** Conclusions

3.1 The approach of European Data Protection Authorities to the "consent or pay" model

In recent weeks, the debate surrounding the "consent or pay" model has been actively unfolding within the decision-making bodies of several European Data Protection Authorities. This section seeks to provide an updated account of their positions, based on the latest publicly available information.

Especially in relation to complex and rapidly evolving issues such as this – often initially addressed at a purely theoretical level – it becomes crucial to closely examine the decisions and guidance issued by supervisory authorities. By applying legal principles to specific factual contexts, these decisions offer valuable insights into how abstract concepts are translated into practice. Indeed, the measures and rulings adopted by the DPAs allow us to frame the issue from a practical and concrete perspective, helping to uncover the underlying rationale that informs their stance on particular aspects of the debate. In this way, the analysis of such decisions not only enhances our understanding of the authorities' current positions but also provides a clearer view of how legal norms are interpreted and enforced in real-world scenarios.[298]

[298] Reference is also made to the map created by Marco Scialdone to verify the positions of European supervisory authorities on pay or consent with their newly released cookie guidelines. The map is also useful for understanding how, within the European Union, various authorities either oppose or partially support the positions of the EDPB. The map is available at the following link: Pay or Consent - Scialdone.

3.1.1 The ICO's approach

The ICO's guidance[299] on "consent or pay" represents a regulatory intervention that, while reaffirming the centrality of freely given consent under UK GDPR, adopts a more permissive stance compared to the EDPB's position[300]. This divergence, though not creating a substantive legal gulf, carries significant implications for interpretation and enforcement.

The ICO, while insisting that consent must be free, specific, informed, and unambiguous, takes a more optimistic view of the potential compliance of "consent or pay" models, offering a flexible assessment framework, in which factors such as power imbalance, appropriateness of the fee, equivalence between options, and adherence to "privacy by design" are balanced on a case-by-case basis.[301] This approach, though rooted in data protection principles, implicitly conveys that the model can be made compliant, provided that organizations proactively document their assessments and corrective measures.[302]

By contrast, the EDPB adopts a more restrictive view[303], stating that, in most cases, large online platforms cannot ensure valid consent when the only choice is between paying a fee or consenting to data processing for personalized advertising. This position is premised on the assumption that power imbalances are structural and difficult to overcome, especially in markets characterized by network effects, high switching costs, and limited real alternatives.

A first critical reflection concerns the ICO's "can do" tone. While the intent is to support innovation and provide businesses with workable guidance, it risks underestimating the

[299] The Information Commissioner's Office (ICO) is the United Kingdom's independent authority responsible for upholding information rights, including the enforcement of data protection legislation such as the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It should be underlined that the UK has begun setting out a series of policy papers which outline a strategy aimed at moving away from the constraints and obligations of European data protection law. This approach promotes reducing barriers to responsible innovation, lowering compliance burdens for businesses, enhancing outcomes for individuals, facilitating trade and cross-border data flows, improving public services, and reforming the Information Commissioner's Office. In essence, the underlying philosophy seeks to simplify the regulatory framework and stimulate innovation, even if this may come at the expense of data protection safeguards.

[300] See EDPB (2024), Opinion 08/2024 on valid consent in the context of consent or pay models implemented by large online platforms, and paragraph 1.5.2 of the present work.

[301] For a proper understanding of the principle of privacy by design, see Chapter 1 and the works of Dr. Ann Cavoukian.

[302] On 23 January 2025, the Information Commissioner's Office published guidance on the use of personal data within a 'consent or pay' business model, following a public consultation on its draft proposals. The guidance acknowledges that it is possible to implement such a model in compliance with the UK GDPR and the PECR, although it highlights the inherent complexity and challenges involved in achieving compliance.

[303] Ibid.

structural nature of power asymmetries in the digital market. The guidance acknowledges that market dominance can create power imbalances, yet suggests that such imbalances might be corrected through alternative options or appropriate pricing. However, this perspective may be overly optimistic, particularly where exit barriers are not merely economic but also social, relational, and informational.

Moreover, the ICO's emphasis on the appropriateness of the fee as an alternative to consent raises questions about the method of evaluation. The guidance explicitly excludes basing the fee on business costs or advertising revenue losses; instead, the "appropriate fee" should reflect the value consumers place on not sharing their data for personalized advertising. While this is theoretically aligned with the logic of freely given consent, it faces practical challenges: measuring such subjective valuations objectively is difficult, particularly in the absence of competitive markets for privacy. The lack of concrete benchmarks risks encouraging opportunistic interpretations by platforms.

Another critical aspect relates to the equivalence between the "consent" and "pay" options. The ICO states that the core service must remain equivalent under both options, allowing for differences in supplementary features. However, the boundary between "ancillary benefits" and substantive changes to the service is not clearly defined. This ambiguity leaves room for platforms to subtly steer users toward consent by making the paid alternative less attractive, not only economically but functionally. The risk is that an ostensibly free choice is in fact engineered through design strategies or indirect penalties.

The Information Commissioner's Office also requires choices to be presented transparently and without manipulative design practices: this focus aligns with broader European concerns about choice architecture's role in shaping user behavior.[304]

Yet, the absence of prescriptive standards or concrete examples of what constitutes a violation weakens the normative force of the guidance, leaving significant interpretive discretion.[305]

In summary, the ICO's guidance reflects a tension between protecting personal data and preserving platform business models. The proposed "case-by-case" approach risks shifting the compliance burden entirely onto organizations, without a sufficiently clear legal

[304] Inge Graef, (2023). The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law.

[305] Ali Talip Pınarbaşı, (2025). Understanding the ICO guidance on 'Consent or Pay' in the UK, Didomi Blog.

framework to ensure consistent and predictable assessments. This could erode effective protection of data subjects, particularly in contexts of informational and market asymmetry. A final observation concerns the implicit regulatory divergence between the UK and the EU emerging from the ICO-EDPB contrast. While both authorities affirm the principle of freely given consent, the ICO's more permissive stance risks creating a regulatory "forum shopping" effect, where platforms may prefer UK jurisdiction to benefit from a more flexible regime.[306]

This scenario raises questions not only about the protection level for UK users but also about the coherence of the post-Brexit digital market: its permissive tone and reliance on organizational self-assessment risk diluting the substantive protection of data subjects' rights. A more prescriptive approach, with clearer safeguards against structural power imbalances and manipulative design, would likely be necessary to achieve a better balance between business freedom and fundamental rights.

3.1.2 The Norwegian Data Protection Authority's approach

The Norwegian Data Protection Authority [307] has emerged as one of the most critical voices against the "pay or okay" model[308], expressing significant concerns regarding its compatibility with the General Data Protection Regulation. In its view, this approach undermines the voluntariness and freedom of consent required under Article 7 GDPR, as individuals may be effectively coerced into accepting data processing in exchange for access to essential services or content. The Authority has therefore taken a firm stance, arguing that such practices fail to meet the standard of valid consent under EU data protection law.[309]

---

[306] Barbora Korcova, (2025). Paying for Privacy? Understanding the ICO's 'Consent or Pay' Rules.

[307] The Norwegian Data Protection Authority, known in Norwegian as *Datatilsynet*, is the national supervisory authority responsible for enforcing data protection laws in Norway. It was established in 1980 following the enactment of the Data Register Act of 1978, one of the earliest data protection laws globally. The authority operates as an independent administrative body under the Ministry of Digitalisation and Public Governance and is headquartered in Oslo.

[308] Usercentrics (2025). New Regulatory Updates for Cookie Use in Norway: What to Know and How to Comply.

[309] Marco Scialdone highlights that the authority is firmly opposed to this model, as indicated in point no. 3 of the Guidance, which states that if access to the website or service is made conditional on consent, the user is not provided with a genuine choice. In such cases, consent will not be considered valid. This applies, among other things, to so-called cookie walls.

This position was further reinforced in its new guidance on cookie consent, published in April 2025, in which the Authority stated that conditioning access to a website or service on consent would deprive users of a genuine choice, thereby rendering consent invalid.[310]
The guidance clarified that this reasoning applies, among other things, to the use of so-called "cookie walls"[311].

3.1.3 The Dutch Data Protection Authority's approach

In a similar vein, the Dutch Data Protection Authority[312] has taken a critical stance toward the use of so-called "cookie walls", arguing that such mechanisms do not provide users with a genuinely free choice.[313] According to the Authority, when access to a website is made conditional on accepting cookies, meaning that visitors cannot access the site unless they give consent, consent cannot be considered freely given. Under the General Data Protection Regulation, consent lacks the element of freedom if individuals are not presented with a real or meaningful choice, or if refusing consent leads to negative consequences. In this perspective, cookie walls undermine the voluntary nature of consent required by Article 7 GDPR.

3.1.4 The Belgian Data Protection Authority's approach

The Belgian Data Protection Authority[314] has similarly raised concerns about the legality of forcing website visitors to accept "non-essential" cookies, or pay for an alternative, in order

---

310 Available at: https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/bruk-av-informasjonskapsler-og-andre-sporingsteknologier/ (last accessed: 4/05/2025).

311 Cookie walls refer to mechanisms that block access to a website or service unless the user consents to the use of cookies, thereby conditioning access on consent. This practice has been widely criticised by data protection authorities for undermining the principle of freely given consent under Article 7 GDPR. Some scholars have recently observed that we are now moving toward a model in which certain media sites impose a double paywall: one for users' data and another for access to quality journalism. According to this view, such practices not only undermine fairness but effectively turn the right not to be tracked into a premium feature.

312 The Dutch Data Protection Authority, known as *Autoriteit Persoonsgegevens* (AP), is the national supervisory authority responsible for enforcing data protection laws in the Netherlands. It was established in 2009, succeeding the *Registratiekamer*, which had been operational since 1989. The AP operates as an independent administrative body under the Ministry of Justice and Security and is headquartered in The Hague.

313 Available at: https://autoriteitpersoonsgegevens.nl/actueel/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies (last accessed: 4/05/2025).

314 The Belgian Data Protection Authority, known as *Gegevensbeschermingsautoriteit* (GBA), is the national supervisory authority responsible for enforcing data protection laws in Belgium. It was established in 2018,

to access content. According to the Authority, such practices do not constitute free consent, as required by the General Data Protection Regulation.[315] In its view, consent cannot be deemed valid if it is conditioned on the acceptance of non-essential cookies or a financial payment, as this undermines the voluntary nature of consent that is central to the GDPR framework.[316]

3.1.5 The Spanish Data Protection Authority's approach

The Spanish Data Protection Authority[317] updated its guidance on cookies on 14 May 2024 to reflect the European Data Protection Board's Opinion 08/2024 on consent in "consent or pay" models. The updated guidance recommends that large online platforms should offer users an "equivalent alternative" to behavioural advertising that does not require payment, such as general or contextual advertising, in order to ensure that consent is freely given and therefore valid under the GDPR. It underscores the importance of the data minimisation principle and highlights that the absence of a free alternative may undermine the validity of consent and lead to potential harm to users.[318]

3.1.6 The Austrian Data Protection Authority's approach

On 25 May 2022, the Austrian Data Protection Authority[319] published a set of FAQs addressing cookies and data protection. In this document[320], the DSB reaffirmed its earlier

succeeding the Privacy Commission, which had been operational since 1998. The GBA operates as an independent administrative body and is headquartered in Brussels.

[315] Yacoob, S. Y. (2024). Cookie Consent Requirements in Belgium.

[316] Available at: https://www.autoriteprotectiondonnees.be/citoyen/themes/internet/cookies#les-sites-web-peuvent-ils-mettre-en-place-des-cookie-walls (last accessed: 4/05/2025).

[317] The Spanish Data Protection Authority, known as *Agencia Española de Protección de Datos* (AEPD), is the national supervisory authority responsible for ensuring compliance with data protection laws in Spain. It was established in 1992 and operates as an independent public body under the Ministry of Justice. The AEPD is headquartered in Madrid.

[318] Available at: https://www.aepd.es/guias/guia-cookies.pdf (last accessed: 4/05/2025).

[319] The Austrian Data Protection Authority (*Datenschutzbehörde*, DSB) is the national supervisory authority responsible for monitoring and enforcing data protection laws in Austria. Established in 2014 following the entry into force of the Austrian Data Protection Act 2000 (as amended), the DSB operates as an independent public authority and is based in Vienna.

[320] Available at: https://dsb.gv.at/download-links/FAQ-zum-Thema-Cookies-und-Datenschutz.htm

position, stating that, in principle, it is permissible to offer users the option to pay for access to a website as an alternative to providing consent for the processing of personal data. This stance suggests a degree of openness toward "consent or pay" models, provided that the conditions for valid consent under the General Data Protection Regulation are met.

3.1.7 The French Data Protection Authority's approach

The French Data Protection Authority[321] was among the first European supervisory authorities to take a strict stance against the use of cookie walls, initially asserting that such practices were always unlawful, as they prevented users from accessing a website or service without accepting cookies. This uncompromising position left no room for alternatives. Following this interpretation, an appeal was brought before the French *Conseil d'État*, which ruled that the CNIL, through non-binding instruments such as guidelines, could not effectively create new legal obligations, invoking the principle of legality. As a result, the French Data Protection Authority was compelled to partially revise its position, although further developments on the matter are still awaited. The CNIL subsequently adopted guidelines[322] similar to those issued by the Italian Data Protection Authority, yet with an even more pragmatic and realistic approach. While the Italian regulator stated that a cookie wall could only be lawful if users were offered an "equivalent alternative" to access the service without consenting to cookies, the CNIL went further by clarifying that this alternative must be assessed in light of the principle of fairness. This emphasis on fairness, requiring the alternative to be not only functionally equivalent but also substantively fair and reasonable, represents an important criterion in evaluating the lawfulness of "pay or okay" models.[323]

(last accessed: 4/05/2025).

[321] The French Data Protection Authority, known as Commission Nationale de l'Informatique et des Libertés (CNIL), is the independent public authority responsible for ensuring data protection compliance in France. It was established in 1978 under the Data Protection Act (Loi Informatique et Libertés) and is headquartered in Paris.

[322] Available at: CNIL - Cookies Guidelines (last accessed: 4/05/2025).

[323] On December 12, 2024, in response to numerous complaints from data subjects, the French Data Protection Authority (CNIL) issued orders to website publishers to modify their cookie banners, which were deemed misleading. For further details, please refer to: CNIL - Formal Notice 2024.

3.1.8 The German Data Protection Authority of Lower Saxony's approach

On May 17, 2023, the Data Protection Authority of Lower Saxony in Germany[324] issued a position on the application of "pay or consent" models, stressing the importance of providing users with the ability to grant granular consent rather than a blanket or generalized consent. The LfD emphasized that such models must align with the principles of the General Data Protection Regulation, particularly the requirements of informed and explicit consent. According to the authority, offering users the opportunity to consent to specific data processing activities, rather than merely consenting to a broad range of activities, ensures greater transparency and enhances the control users have over their personal data. This position underscores the LfD's commitment to upholding the fundamental rights of individuals under the GDPR, even in contexts where a payment or consent-based access model is utilized.[325]

3.1.9 The Italian Data Protection Authority's approach

The Italian Data Protection Authority[326] is still investigating the use of paywall and cookie wall systems, with the investigation having begun in October 2022.[327] In recent months, numerous online media outlets, websites, and companies operating in the television sector have implemented systems that condition access to content either on the subscription to a service (the so-called paywall) or, alternatively, on users' consent to the installation of cookies and other data tracking tools (referred to as cookie walls). Following reports and complaints, the Garante is examining these practices within the framework of current legislation, to assess

[324] The Data Protection Authority of Lower Saxony (Landesbeauftragte für den Datenschutz Niedersachsen, LfD) is an independent authority responsible for monitoring and enforcing data protection laws in the German state of Lower Saxony. It was established under the Federal Data Protection Act (BDSG).

[325] Available at: https://privacy-web.nl/wp-content/uploads/po_assets/866009.pdf (last accessed: 4/05/2025).

[326] The Garante per la Protezione dei Dati Personali, often simply referred to as the Garante Privacy, was established by Law No. 675 of December 31, 1996, with the aim of protecting individuals' rights, freedoms, and dignity in relation to the processing of personal data.

[327] For further information, see Doc-Web 9815415 (Garante Privacy).

whether any regulatory action is warranted.[328] Although the Authority has not yet issued an official position, it has acknowledged that European personal data protection legislation does not, in principle, prohibit website operators from conditioning access to content on users' consent for profiling purposes (through cookies or other tracking technologies), or alternatively, on payment.[329]

On May 5, 2025, the Italian Data Protection Authority, acknowledging both the growing significance of the phenomenon and its potential implications for the rights and fundamental freedoms of a vast number of data subjects, launched a public consultation[330] aimed at evaluating the legal validity of consent collected for profiling purposes under the "pay or ok"[331] model, particularly when consent is obtained by multiple data controllers, most notably news publishers.

Central to the debate is whether the consent provided by users under such a scheme can genuinely be considered "freely given" within the meaning of applicable data protection rules. Indeed, empirical observations indicate that a substantial proportion of users, eager to access content, services, or functionalities offered without direct monetary payment, tend to consent to the processing of their personal data without fully grasping the long-term consequences of their choice.[332]

Notably, the Authority's reasoning suggests that an isolated institutional response, limited to adopting individual decisions against companies under current investigation, may be insufficient and inadequate in addressing the broader structural issues at stake. Such isolated enforcement actions may fail to provide a sustainable and effective alternative capable of balancing competing interests: on one hand, the legitimate economic and operational needs of businesses, especially in the publishing sector and, by extension, the imperative to uphold a robust and pluralistic flow of information; on the other hand, the fundamental requirement to ensure compliance with data protection principles safeguarding the rights of millions of individuals.

---

[328] Gazzella, S. (2025). Cookie Paywall, fra silenzi e scuse.

[329] For further information, see Doc-Web 9816536 (Garante Privacy).

[330] Available at: Pay or Ok - Consultazione Pubblica.

[331] As discussed throughout this dissertation, this phenomenon is referred to interchangeably as "consent paywall", "Pay or Ok", "Consent or Pay", or "Pay or Consent".

[332] See also the discussion on *consent fatigue* in Chapter 1.

Simultaneously, the Authority's initiative explicitly aims to avoid a purely punitive or sanction-focused approach, which could risk undermining the prevailing market model adopted by publishers and other affected controllers, while failing to articulate a viable alternative that adequately reconciles economic imperatives, the free circulation of information, and the fundamental right to data protection.[333]

The public consultation, open to all stakeholders, is designed to collect substantive contributions and insights towards identifying technical and operational solutions to this complex dilemma. Among the core issues under examination are:

- whether the "pay or ok" model is compatible with the objectives and underlying rationale of the current legal framework governing consent to personal data processing. Specifically, the consultation questions whether consent, required to be free and informed under the law, can truly meet these standards in scenarios where individuals, faced with a binary choice, either pay an economic fee or accept comprehensive data processing as a condition of access. In particular, concerns are raised about the nature of a single, bundled consent, mandatorily covering a broad range of profiling and marketing purposes, including the automatic sharing of data with hundreds of third parties, many of whom may be unknown or only partially identifiable to the user. This form of consent, necessarily aggregated and provided without meaningful opportunity for granular choice, may deprive data subjects of the predictability and effective control over their personal data that the legal framework seeks to ensure;
- whether – and if so, what – possible alternatives to the current binary "pay or ok" structure could be envisaged, alternatives that would impose a lesser impact on individuals' privacy rights. Such alternatives would ideally entail a lesser intrusion into privacy, reducing the scope or intensity of personal data processing or even avoiding data processing altogether, thus better preserving the essence of the right to data protection;
- which measures or mechanisms could effectively ensure that users are provided with clear, comprehensible, and predictable information regarding the consequences of their

[333] Several commentators argue that the decision to initiate a public consultation on the issue, rather than pursuing an immediate sanctioning approach, can be attributed to the fact that many of the data controllers involved are publishers. According to this line of reasoning, it is precisely the strategic importance of the publishing sector that has led the Authority to adopt a more cautious, consultative stance. These commentators further observe that "assessing the lawfulness" of a specific data processing practice is, by its nature, a task typically reserved for regulatory enforcement rather than public consultation. They question whether a public consultation is the appropriate tool in this context: if the practice is lawful, it should not require the identification of alternative models; conversely, if it is unlawful, the Authority should act directly by enforcing the applicable rules rather than seeking alternatives through consultation

consent. This relates both to their right to access a specified quantity and quality of editorial content, as well as other services or functionalities contingent on their decision.

The consultation also emphasizes the legal requirement that consent must be not only free and specific but also properly informed, ensuring that individuals are fully aware of the implications of their consent, thereby upholding the principles of autonomy, specificity, and awareness integral to valid consent under data protection law.[334]

Through this multifaceted inquiry, the Authority seeks not only to clarify the boundaries of lawful consent in the context of emerging business models but also to encourage a broader reflection on how to reconcile economic innovation, media sustainability, and the inviolable right to personal data protection in the digital age.

Among the various issues at hand, it is crucial to highlight another problematic practice that can be legitimately contested against publishers: the practice of charging users twice. The first charge occurs when users access the website. Upon entering, they are asked to accept cookies in order to access content, with the implicit message that they must either pay with their personal data or pay with money. Once this condition is accepted, users reasonably assume they have fulfilled their payment and can now access the newspaper.

However, in order to read specific articles, another payment is requested, often in the form of a subscription. The data provided, therefore, only grant access to the homepage and do not extend to the full content of the website.[335] It is noteworthy that, coincidentally, all major publishers adopted this dual-payment model on the exact same day, suggesting a coordinated strategy rather than an isolated market behaviour.

The Italian Supreme Court, in ruling no. 17278/2018, has acknowledged that, in certain cases, it is legitimate to condition access to a service on the user's consent for marketing purposes, provided this requirement is part of the business model. However, the Court

---

[334] In formulating its approach, the Authority has drawn upon a number of foundational legal and policy instruments, including: Opinion 04/2012 on Cookie Consent Exemption, adopted on 7 June 2012 by the Article 29 Working Party (WP29); WP29 Working Document 02/2013 providing guidance on obtaining consent for cookies, adopted on 2 October 2013; the WP29 Guidelines on Consent under Regulation (EU) 2016/679, adopted on 10 April 2018 and endorsed by the European Data Protection Board (EDPB) on 25 May 2018, subsequently replaced by the EDPB's Guidelines 05/2020 on Consent under Regulation 2016/679, adopted on 4 May 2020; the WP29 Guidelines on Transparency under Regulation (EU) 2016/679, revised on 11 April 2018; the letter adopted by the EDPB on 13 December 2023 in response to the European Commission's Cookie Pledge initiative; and the EDPB Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, adopted on 17 April 2024.

[335] Such a practice is fundamentally inequitable and gives rise to significant doubts, particularly from a competition law perspective.

stipulated that such practices are only deemed lawful if the goods or services offered are fungible and easily available elsewhere.

The core issue, then, lies in the fact that if all publishers adopt the same approach, the concept of an "alternative good" effectively disappears. As a result, the very condition that the Supreme Court regarded as exceptional and acceptable no longer holds.[336]

3.2 Meta found in breach of the Digital Markets Act: European Commission's April 2025 Decision

On April 23, 2025, the European Commission determined that Meta's pre-November 2024 "consent or pay" model violated the Digital Markets Act.[337] This recognition is significant: it confirms that dominant platforms (who shouldn't coerce users in any case, though the DMA targets gatekeepers specifically) cannot impose a binary choice between paying money or handing over personal data.[338]

This decision follows a broader context in which data protection authorities raised serious concerns about the significant risks such a model poses to individuals' informational self-determination, despite its adoption by news outlets and publishers as a means to generate online revenue.[339] Their concerns proved well-founded. Meta's "pay or consent" model was introduced in response to earlier determinations by the Irish DPA, which concluded that the company could not rely on legitimate interest or contractual necessity as legal bases to process personal data for personalised advertising.[340]

The Commission is now reviewing Meta's so-called "third option", introduced in November 2024. According to the Commission's press release, this alternative supposedly relies on less personal data for advertising. Yet reducing the amount of data collected doesn't solve the

[336] Some argue that, for these reasons, the illegitimacy of these practices is evident. It is difficult to discern what additional valuable insights might emerge from a public consultation on this issue.

[337] See also above, paragraph 2.4.

[338] European Commission, Press Release, available at: Apple and Meta - DMA.

[339] Martínez, A.R. (2025). The DMA's Teeth: Meta and Apple Fined by the European Commission. Kluwer Competition Blog.

[340] For further details, see Data Protection Commission announces conclusion of two inquiries into Meta Ireland.

fundamental legal issue. Nor does it alter the underlying imbalance of power embedded in the model.[341]

It's worth revisiting what this "third option" entails:

- It only becomes available after a user has already "consented" – though this consent arguably falls short of GDPR standards.[342]
- It offers "less personalized" ads, but with disruptive and manipulative ad breaks clearly engineered to frustrate the user, pushing them back toward full profiling.
- It doesn't function as a genuine alternative (and *genuine* is the operative word) to consent.[343] Instead, it's a downgraded experience presented *after* consent, rather than a rights-based choice at the outset.

In other words, this is not a solution: it is the same coercive approach, simply repackaged across different interfaces and framed in language that merely appears more respectful of user rights.

And herein lies the risk: by treating this "third option" as a separate, pending assessment, the Commission inadvertently signals that compliance can be achieved through design tricks rather than through the substantive structural changes the law demands.

We've seen this pattern countless times. It's a form of "compliance-washing" – superficial adjustments that maintain exploitative practices at their core.

---

[341] Davies, G. (2025). Consent or pay. Transforming internet users from products into customers. Journal of European Consumer and Market Law.

[342] The Digital Markets Act incorporates the standard for consent established under the General Data Protection Regulation. It is plausible that the European Commission found Meta's binary choice model to constitute coercive consent, drawing significantly on the European Data Protection Board's Opinion 08/2024 regarding "consent or pay" models under the GDPR. However, the direct application of this specific interpretation of the GDPR to the DMA raises important questions. This approach warrants careful examination, particularly in light of the Court of Justice of the European Union's recognition that valid consent may still be obtained in a context of market dominance, provided that an alternative option involving an "appropriate fee" is available.

[343] Recital 36 of the Digital Markets Act (DMA) requires the provision of a "less personalised but equivalent alternative" for users who do not consent. The European Commission appears to have interpreted this requirement as implying the obligation to offer a free alternative, thereby considering Meta's paid ad-free subscription insufficient to meet the standard. This interpretation arguably represents the most innovative, or perhaps legally contentious, aspect of the Commission's inferred reasoning. Notably, the Court of Justice of the European Union has explicitly acknowledged the possibility of imposing an "appropriate fee" under the GDPR, and the text of the DMA does not expressly prohibit charging users for the alternative. Framing freeness as a mandatory requirement under the DMA thus seems to reflect not a strict application of the legislative text, but rather an alignment with the policy preferences articulated by the European Data Protection Board in the context of the GDPR.

And it works, precisely because it creates the illusion of progress while preserving harmful dynamics. Meanwhile, companies still express outrage when fined for blatantly misleading behavior.[344]

The legal framework leaves no room for doubt:

- Under the GDPR, consent must be freely given, specific, informed, and granted without detriment.
- Under the DMA, gatekeepers are obliged to secure valid consent (as also defined by the GDPR) and to ensure users who refuse consent can still access services without degradation.

It is necessary to move beyond the notion that minor adjustments to a business model amount to genuine compliance. Consent cannot be considered valid when refusal results in negative consequences or when individuals are subtly pressured into providing agreement. Furthermore, power asymmetries are not eliminated simply by shifting the point of pressure to a subsequent interface. The European Commission's initial finding against Meta represents a correct interpretation of the applicable legal framework. However, further action is needed to recognize the so-called "third option" for what it effectively constitutes: not a compliant alternative, but a continuation of coercive practices.[345]

At the same time, it is worth noting that the European Commission's recent enforcement actions have reignited an important debate on the intersection between competition law and data protection. While the DMA is not a data protection law, its obligations on so-called "gatekeepers" inevitably affect the governance of personal data. Recital 12 of the DMA clarifies that its provisions do not override other EU laws, including the GDPR, thus requiring a harmonious interpretation of both instruments. However, the simultaneous application of these regulations risks creating legal tensions, particularly when enforcement responsibilities are divided between the European Commission, as the DMA enforcer, and national data protection authorities, responsible for the GDPR.

[344] Palumbo, R. (2025). Modello Pay or consent: le implicazioni privacy delle sanzioni della Commissione UE. Agenda Digitale.

[345] Martínez, A.R. (2025). The DMA's Teeth: Meta and Apple Fined by the European Commission. Kluwer Competition Blog.

This structural divergence is further amplified by the GDPR's decentralized "one stop shop" mechanism[346]: intended to streamline compliance, this mechanism has faced criticism for delays and perceived leniency, particularly toward large technology companies headquartered in jurisdictions like Ireland or Luxembourg. The Court of Justice of the European Union, in C-645/19, emphasized the need for cooperation among authorities while affirming that other national regulators retain the right to intervene when fundamental rights are at stake.
This tension between economic models and legal safeguards highlights broader challenges in aligning competition law with data protection: while the DMA enhances certain user rights, such as data portability [347] and transparency in profiling practices[348], the integration of these rights within a coherent regulatory framework remains incomplete.
As previously mentioned, the European Commission is currently evaluating whether the modifications introduced by Meta satisfy the compliance obligations set out in Article 5(2) of the Digital Markets Act. If the Commission adheres to the reasoning developed by the European Data Protection Board and applies a rigorous assessment, further regulatory challenges for Meta appear likely. Given the provisional nature of the newly implemented features, which have yet to be formally assessed under Article 5(2) DMA, the non-compliance decision issued against Meta raises questions regarding its alignment with the procedural requirements established in Article 29 DMA.
According to Article 29(5) DMA, a non-compliance decision must instruct the gatekeeper to cease the infringement within an appropriate deadline and to provide details on how compliance will be achieved. In contrast to the Commission's non-compliance decision against Apple for a violation of Article 5(4) DMA, the decision concerning Meta does not explicitly include an order to cease the unlawful conduct. As a result, while Meta's "pay or consent" subscription model will ultimately need to be withdrawn, it is not subject to the same 60-day compliance deadline imposed in Apple's case. Consequently, the non-compliance decision is expected to require supplementary enforcement measures, either through the issuance of a new non-compliance decision or an amendment of the existing one. Furthermore, since Article 5(2) DMA cannot be addressed through specification

[346] It designates the supervisory authority of the main establishment of a data controller or processor within the EU as the lead authority for cross-border data processing activities, facilitating coordinated decision-making among supervisory authorities.

[347] Recital 59 of DMA.

[348] Recital 72 of DMA.

proceedings under Article 8(2), there is no procedural avenue for the Commission to adopt non-punitive implementation measures to secure compliance.[349]

3.3 An alternative third option beyond the "consent or pay" model

The emergence of artificial intelligence tools as a "third option" in the evolving landscape of online consent mechanisms offers a compelling alternative to the prevailing "consent or pay" dichotomy, promising significant positive effects on user awareness, autonomy, and trust in digital ecosystems, while potentially reshaping corporate accountability and regulatory dynamics in an era of increasing datafication. Under the current model, users are often compelled to either accept expansive data collection practices - embedded in lengthy, opaque privacy policies - or pay for premium services to avoid such intrusions, a binary choice that exploits information asymmetries and undermines meaningful consent.[350]

AI-driven tools could transcend this paradigm by analyzing complex legal texts and technical frameworks in real time, delivering concise, personalized summaries that elucidate the implications of consent decisions; for example, an AI system might inform a user that "agreeing to this policy allows your location data to be shared with third-party advertisers for up to five years", thereby transforming abstract terms into tangible consequences.[351] This enhanced transparency addresses a critical barrier: users frequently acquiesce to terms they do not comprehend due to cognitive overload, with studies suggesting that the average privacy policy requires a reading level far exceeding that of most internet users.[352] Beyond mere comprehension, such tools could empower users with granular control, enabling them to selectively approve specific data uses, consenting to analytics but not behavioral profiling,

---

[349] Martínez, A.R. (2025). The DMA's Teeth: Meta and Apple Fined by the European Commission. Kluwer Competition Blog.

[350] Zuboff, S., & Schwandt, K. (2019). The age of surveillance capitalism: the fight for a human future at the new frontier of power. Profile Books.

[351] In a similar vein, see Antonio Punzi in "Commerciabilità dei dati personali. Profili economici, giuridici, etici della monetizzazione", who suggests that the dialogical dimension of consent in data processing could potentially be reimagined through interactions with artificial intelligence systems. Punzi envisions AI capable not only of explaining the potential uses of personal data but also of actively inquiring about users' preferences, thereby collecting their choices in a way that ensures ongoing, tailored execution each time they access the internet. Such interaction, he argues, would not necessarily need to occur upon every website visit, but could instead be carried out periodically by an intermediary agent, operating automatically yet programmed in accordance with parameters defined by competent authorities, in line with constitutional principles.

[352] See also the discussion on *consent fatigue* in Chapter 1.

rather than facing the all-or-nothing ultimatums typical of current interfaces, a limitation that is criticized as rendering consent a hollow formality.[353]

Moreover, AI systems could adapt dynamically, responding to user queries with tailored clarifications, such as explaining the difference between "necessary" and "optional" cookies, thereby fostering a dialogic rather than unilateral consent process, which aligns with principles of user-centered design. This interactivity could bolster trust, a cornerstone of technology acceptance models, as users feel less like passive subjects and more like active participants in data governance.[354] The ripple effects extend further: by making data practices more visible, AI tools might pressure companies to simplify or ethically refine their policies to avoid user backlash flagged by unflattering AI-generated summaries, indirectly promoting accountability in a manner similar to market-driven self-regulation. For instance, a firm might reconsider excessive data retention if an AI consistently highlights it as a point of user concern, nudging industry standards toward greater fairness. From a societal perspective, widespread adoption of such tools could democratize digital literacy, leveling the playing field for non-expert users who lack the time or expertise to navigate privacy settings, a disparity highlighted in research on the digital divide.[355]

Critics might argue that implementation challenges, such as algorithmic bias, corporate resistance, or the risk of oversimplification, could undermine these benefits, yet these hurdles are not insurmountable; bias can be mitigated through rigorous auditing, and corporate pushback might wane if consumer demand for transparency grows.[356] Furthermore, the technology's scalability offers a practical advantage: once developed, AI tools could be integrated into browsers, apps, or operating systems, requiring minimal user effort while delivering consistent, real-time insights across platforms, a feat unachievable by static consent notices. In educational terms, this could cultivate a more informed populace over time, as repeated exposure to AI explanations builds intuitive understanding of data rights, potentially reducing the "privacy paradox" wherein users express concern yet fail to act.

---

[353] Solove, D. J. (2021). The Myth of the Privacy Paradox. George Washington Law Review 1.

[354] McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. I/S: A Journal of Law and Policy for the Information Society.

[355] Kuhn, C., Khoo, S.-M., Czerniewicz, L., Lilley, W., Bute, S., Crean, A., Abegglen, S., Burns, T., Sinfield, S., Jandrić, P., Knox, J., & MacKenzie, A. (2023). Understanding digital inequality: A theoretical kaleidoscope. Springer.

[356] Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence.

Finally, this "third option" reimagines consent not as a transactional burden but as an ongoing, informed negotiation, aligning with ethical ideals of autonomy and agency in the digital age, and offering a pathway beyond the coercive trade-offs of "pay or consent" toward a more equitable, user-centric internet.

3.4 Balancing data protection and market efficiency: towards a coherent regulatory approach

While the primary objective of protecting individuals' data rights must be upheld, data protection provisions can be designed in a way that minimizes their impact on competition and innovation. Data protection regulations play a crucial role in safeguarding individual welfare and establishing trust between users and businesses. However, complying with these obligations can increase the costs of entry and operation, particularly for smaller undertakings[357]. Data protection policies that limit incentives to share personal data or restrict the use of data collected by third parties may further entrench the positions of dominant players and reduce opportunities for innovation. This does not imply that competition concerns should outweigh the need to protect data rights; rather, there is room to reconsider the design of data protection regimes to mitigate negative impacts on competition while continuing to safeguard individuals' rights.

On the other hand, there is increasing recognition that the level of data protection a company offers holds value for consumers and can be considered a non-price aspect of competition. Understanding how undertakings voluntarily enhance data protection to gain a competitive edge is crucial for accurately analyzing market dynamics.

Overall, there is a clear need for greater cooperation between competition and data protection authorities: collaboration between regulatory bodies can assist policymakers in identifying data protection policies that minimize competition distortions, developing data-focused competition remedies that preserve data rights, and determining which antitrust cases should be pursued in situations involving excessive data collection or exploitation of consumers.

[357] In this regard, the European Commission confirmed in March 2025 its intention to streamline the application of the General Data Protection Regulation by easing certain obligations for companies with fewer than 500 employees. In particular, it announced plans to revise Article 30 GDPR, which governs records of processing activities. This development represents a significant step toward reducing administrative burdens and promoting regulatory simplification for small and medium-sized enterprises.

What emerges from the current state of analysis is that ensuring the effectiveness and sustainability of such models necessitates coordinated action among institutions. The principle of sincere cooperation under Article 4(3) of the Treaty on European Union obliges EU institutions and Member States to collaborate in enforcing EU law. This principle calls for substantive and procedural alignment between the Commission and national authorities to prevent fragmented or inconsistent enforcement. Recent enforcement challenges under the GDPR's decentralized model have reignited discussions about whether stronger centralization, potentially granting the Commission a more prominent role in cross-border cases, might be necessary.

The relationship between competition law and data protection also requires careful navigation: the CJEU and national courts, such as Italy's Council of State, have established that competition authorities assessing data protection compliance within antitrust proceedings must defer to the expertise and authority of data protection regulators. This principle ensures that regulatory domains remain distinct, while fostering cooperation to achieve coherent outcomes.

Ultimately, the Commission's actions against Meta and Apple signal a broader shift toward integrated governance of digital markets, recognizing that privacy, competition, and access to services cannot be treated as isolated policy spheres. The evolving regulatory landscape suggests that sustainable digital business models must reconcile economic imperatives with the fundamental rights of users. The introduction of less intrusive advertising models and the push for more transparent, equitable practices reflect an emerging consensus that effective regulation requires synergy across legal frameworks.

By challenging the "pay or consent" model, the European Commission not only questions the validity of consent under current practices but also sets a precedent for future regulation of data-driven business models. This evolving dynamic underscores the need for balanced, integrated approaches to ensure that innovation, user autonomy, and fundamental rights coexist within Europe's digital economy.[358]

[358] Martínez, A.R. (2025). The DMA's Teeth: Meta and Apple Fined by the European Commission. Kluwer Competition Blog.

3.5 Conclusions

This dissertation has sought to provide a comprehensive exploration of the evolving legal concept of consent in the digital age, situating it within the broader context of technological change and the emergence of new online business models. By tracing the shifting boundaries of consent, from a traditional legal safeguard to a contested site where fundamental rights, economic interests, and technological innovation collide, it has aimed to offer a nuanced perspective on how consent is being reinterpreted in both regulatory and practical terms. The analysis has demonstrated that the legal framework governing consent cannot be understood in isolation but must be assessed in light of the complex interplay between data protection, competition law, and market dynamics.

The future of "consent or pay" models will hinge on their ability to reconcile compliance with Article 4(11) GDPR's requirements with the broader need for fairness, accessibility, and inclusivity in the digital marketplace. Critiquing such models without offering viable alternatives risks driving platforms toward even more exclusionary practices, such as "pay or pay" schemes, where users are forced to sacrifice either their privacy or their financial resources. This shift could undermine user trust, exacerbate digital inequalities, and threaten the principle of an open and accessible internet. Indeed, dismantling the "freemium" model could disproportionately affect economically disadvantaged groups, effectively restricting access to essential online services and amplifying the digital divide.

Achieving a fairer balance demands greater regulatory clarity, closer cooperation between regulatory authorities, and a willingness to engage in a dialogue between legal regimes. Privacy must not be treated as a self-contained domain but must be understood as part of a broader ecosystem. A possible path forward lies in diversifying the range of choices available to consumers and empowering them through greater transparency. Emerging technologies, such as AI-driven tools capable of providing real-time, comprehensible explanations of consent implications, could help bridge the gap between legal formalism and genuine user understanding.

Ultimately, the question is whether data protection remains an isolated realm or becomes a region in a larger order, one that must dialogue with other normative domains to avoid conflicts of fundamental rights. Only by fostering this dialogue we can construct a regulatory approach that balances privacy, innovation, market efficiency, and fairness, thereby ensuring a sustainable and rights-respecting digital economy.

Recent decisions, such as those concerning Meta and Apple in April 2025, exemplify the European Commission's concrete application of its enforcement powers under the DMA: these rulings signal an important step in the integration of competition law and data protection regulation, showcasing the evolving role of the Commission in addressing the intersection of market dynamics and fundamental rights. Such decisions provide valuable precedents for both gatekeepers and future regulatory coordination between the Commission, national competition authorities, and data protection bodies, highlighting the need for a cohesive regulatory framework that ensures fairness and protects users' rights.

Bibliography

Akman, P. (2022). A Web of Paradoxes: Empirical Evidence on Online Platform Users and Implications for Competition and Regulation in Digital Markets. Virginia Law and Business Review.

Alpa, G., & Resta, G. (2019). Le persone e la famiglia. Vol. 1: Le persone fisiche e i diritti della personalità. Torino.

Arthur Cox LLP. (2024). Critical Analysis of EDPB Opinion 08/2024.

Baltag, A., & Leszczynska, A. (2024). "Can I have it non-personalised?" An Empirical Investigation of Consumer Willingness to Share Data for Personalised Services and Ads. Journal of Consumer Policy.

Basunti, C. (2020). La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali. Contratto e Impresa.

Battelli, A. (2022). Negoziabilità dei dati personali e modelli di valorizzazione economica. Rivista di Diritto dell'Impresa.

BEUC. (2025). Assessment of Meta's Latest Pay-or-Consent Policy for Facebook and Instagram Users, January 2025.

Bolognini, L., Covello, L., & Fiordalisi, G. (2024). Admissibility of the "Pay or Consent" Model.

Borgobello, M. (2023). Manuale di diritto della protezione dei dati personali, dei servizi e dei mercati digitali. Milano.

Bravo, F. (2017). Il consenso e le altre condizioni di liceità del trattamento dei dati personali. Bologna, Zanichelli.

Cafaggi, F. (2008). Judicial and Administrative Enforcement in Consumer Protection: The Way Forward.

Caggia, F. (2019). Libertà ed espressione del consenso. Torino, Giappichelli.

Caggiano, I.A. (2018). Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali, in Osservatorio di diritto civile e commerciale.

Carolan, E. (2016). The continuing problems with online consent under the EU's emerging data protection principles. Computer Law & Security Review

Carugati, C. (2023). The 'pay-or-consent' challenge for platform regulators. Bruegel, Analysis 32/2023.

Cavoukian, A. (2009). Privacy by Design: The 7 Foundational Principles. Office of the Information and Privacy Commissioner of Ontario.

Choi, H., et al. (2018). The role of privacy fatigue in online privacy behaviour. Computers in Human Behavior.

CIPL. (2024). The limitations of consent as a legal basis for data processing in the digital society.

Colapietro, C. & Iannuzzi, A. (2017). I principi generali del trattamento dei dati personali e i diritti dell'interessato. Napoli, Editoriale Scientifica.

Craddock, P. (2024). Op-Ed: A Critical Analysis of the EDPB's "Pay or Consent" Opinion.

Cremona, L., Laviola, F., & Pagnanelli, G. (Eds.). (2017). Il valore economico dei dati personali tra diritto pubblico e diritto privato. Milano: Giuffrè.

D'Amico, A. S. (2023). Market Power and the GDPR: Can Consent Given to Dominant Companies Ever Be Freely Given? Utrecht University School of Law Research Paper.

Davies, G. T. (2025). Consent or Pay: Transforming Internet Users from Products into Customers. Journal of European Consumer and Market Law.

De Franceschi, A. (2021). Il "pagamento" mediante dati personali. In Annuario 2021 Osservatorio Giuridico sulla Innovazione Digitale.

De Streel, A., & Monti, G. (2024). Data-Related Obligations in the DMA. Centre on Regulation in Europe (CERRE), Implementing the DMA: Substantive and Procedural Principles, January 2024.

Elvy, S. (2017). Paying for privacy and the personal data economy. Columbia Law Review.

Fabbio, P. (2019). Il diritto della concorrenza in Germania: osservazioni e valutazioni in prospettiva europea. Orizzonti del diritto commerciale, fascicolo 3/2019.

Fabio, B. (2021). Rating reputazionale e trasparenza dell'algoritmo. Il caso "Mevaluate". Diritto dell'informazione e dell'informatica (Il), 2021, n. 6, Giuffrè Francis Lefebvre.

Feinberg, J. (1982). Autonomy, sovereignty, and privacy: Moral ideals in the constitution. Notre Dame L. Rev.

Filpi, G. (2022). Il rapporto tra data protection e diritto antitrust alla luce del caso "Facebook Germany": Analisi e prospettive future.

Finocchiaro, G. (2024). Consenso al trattamento e libertà. Libertà e liceità del consenso nel trattamento dei dati personali. Firenze, Persona e Mercato.

Galli, F. (2023). Reputation Rating and Algorithm Transparency: The Case of "Mevaluate". University of Bologna.

Gentili, A. & Cintio, V. (2018). I nuovi "vizi del consenso". Contratto e impresa.

Giannone Codiglione, G. (2016). Risk-based approach e trattamento dei dati personali.

Gómez Alonso, A. (2024). Competition, Intellectual and Industrial Property Law. Lecture 11/24, Universidad Comillas -ICADE.

Harris, T. et al. (2020). The Social Dilemma. Directed by J. Orlowski. Netflix.

Hartzog, W. & Richards N. (2020). Privacy's Constitutional Moment and the Limits of Data Protection. Boston College Law Review.

Hoefling, S. (2022). The German Facebook Case - Alternative Membership Models as An Approach?

Iamiceli, P. (2024). Consenso al trattamento e giurisprudenza europea. Libertà e liceità del consenso nel trattamento dei dati personali. Firenze, Persona e Mercato.

Inge Graef, (2023). The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law.

Irti, N. (1998). Scambi senza accordo. Rivista trimestrale di diritto e procedura civile.

Jeffrey, M., Maynes, C., Lowry, P. B., & Babb, J. (2014). Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure. Paper presented at the International Conference on Information Systems. Auckland, New Zealand.

Kerber, W. & Zolna, K. K. (2022). The German Facebook Case: The Law and Economics of the Relationship Between Competition and Data Protection Law. European Journal of Law and Economics.

Korvoka, B. (2025). Paying for Privacy? Understanding the ICO's 'Consent or Pay' Rules.

Kosta, E. (2013). Consent in European data protection law. Martinus Nijhoff Publishers.

Krommendij, J. & Zuiderveen Borgesius, F. (2022). How to read CJEU judgments: deciphering the Kirchberg oracle. Eu Law Analysis.

Kuhn, C., Khoo, S.-M., Czerniewicz, L., Lilley, W., Bute, S., Crean, A., Abegglen, S., Burns, T., Sinfield, S., Jandrić, P., Knox, J., & MacKenzie, A. (2023). Understanding digital inequality: A theoretical kaleidoscope. Springer.

Lanier, J. (2011). You Are Not a Gadget: a Manifesto.

Lawler, R. (2023). Ad-Free Instagram and Facebook Is Here – and It's Expensive. The Verge.

Machina Grifeo, F. (2023). Rating reputazionale sul web: il consenso deve riguardare il funzionamento dell'algoritmo. NT+ Diritto.

Manganello, G. (2020). Consent and the illusion of autonomy in EU data protection: the necessary utopia.

Manis, M. L. (2018). La Biobanca Genetica di SharDNA Spa acquistata da Tiziana Life Science PLC. Tutte le tappe della vicenda e le questioni giuridiche da risolvere. Il Sole 24 Ore.

Manson, N. C., & O'Neill, O. (2007). Rethinking informed consent in bioethics. Cambridge University Press.

Martínez, A.R. (2025). The DMA's Teeth: Meta and Apple Fined by the European Commission. Kluwer Competition Blog.

Mazzamuto, S. (2006). Il principio del consenso e il problema della revoca. Libera circolazione e protezione dei dati personali.

McDonald, A. M., & Cranor, L. F. (2009). The Cost of Reading Privacy Policies. Journal of Law and Policy for the Information Society.

Morel, V., Santos, C., Fredholm, V., & Thunberg, A. (2023). Legitimate Interest is the New Consent – Large-Scale Measurement and Legal Compliance of IAB Europe TCF Paywalls. Proceedings of the 21st Workshop on Privacy in the Electronic Society. Copenhagen, Denmark.

Morel, V., Santos, C., Lintao, Y., & Human, S. (2022). Your Consent Is Worth 75 Euros A Year – Measurement and Lawfulness of Cookie Paywalls. 21st Workshop on Privacy in the Electronic Society (WPES '22), Los Angeles, CA, USA, November 2022.

Müller-Tribbensee, T., Miller, K. M., & Skiera, B. (2024). Paying for Privacy: Pay-or-Tracking Walls.

Mursia, M., & Trovato, G. (2021). The commodification of our digital identity: limits on monetizing personal data in the European context. MediaLaws – Rivista di diritto dei media.

Nettesheim, M. (2020). Data Protection in Contractual Relationships (Art. 6(1) (b) GDPR), in The EU General Data Protection Regulation (GDPR).

Nettesheim, M. (2024). EU Data Protection Law and Pay-or-Consent Business Models.

Noronha, L. (2025). Meta's 'Consent-or-Pay' after the European Data Protection Board Opinion 08/2024: Is GDPR Compliance Possible? Tilburg Law School.

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence.

Olivieri, G. (2021). The "Dangerous Relationship" Between Antitrust and Privacy in Digital Markets, Giappichelli.

Orlando S., (2024). Libertà e liceità del consenso nel trattamento dei dati personali. Persona e Mercato, Firenze.

Orlando, S. (2022). Per un sindacato di liceità del consenso privacy. Persona e Mercato, Firenze.

Palumbo, R. (2025). Modello Pay or consent: le implicazioni privacy delle sanzioni della Commissione UE. Agenda Digitale.

Pınarbaşı, A. T. (2025). Understanding the ICO guidance on 'Consent or Pay' in the UK, Didomi Blog.

Pizzetti, F. (2016). Privacy e il diritto europeo alla protezione dei dati personali. Giappichelli.

Podszun, R. (2020). The Consumer as a Market Player: Competition Law, Consumer Choice and Data Protection in the German Facebook Decision.

Podszun, R., & Marsden, P. (2020). Restoring balance to digital competition – Sensible rules, effective enforcement. Konrad-Adenauer-Stiftung e. V.

Poggi, A. & Fabbrizi, F. & Savastano, F. (2023). Social network, formazione del consenso e intelligenza artificiale. Itinerario di un percorso di ricerca di Beniamino Caravita.

Punzi, A. (2024). In Cerrina Feroni, G., Commerciabilità dei dati personali. Profili economici, giuridici, etici della monetizzazione. Il Mulino.

Rawls, J. (1971). *A Theory of Justice.* Harvard University Press.

Resta, G. & Zeno-Zencovich, V. (2018). Will and Consent in the Provision of Services on the Internet.

Ricciuto, V. (2024). Consenso al trattamento e libertà. Consenso al trattamento e liceità. Firenze, Persona e Mercato.

Richards, N. & Hartzog, W. (2019). The Pathologies of Digital Consent. Washington University Law Review.

Rodotà, S. (1995). Tecnologie e diritti. Bologna, Il Mulino.

Sacco, R. (2016). Il contratto. Milano.

Sandel, M. J. (2012). What Money Can't Buy: The Moral Limits of Markets. Farrar, Straus and Giroux.

Santos, C., Bielova, N., & Matte, C. (2020). Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. Technology and Regulation, Tilburg University.

Satariano, A. (2020). Facebook Loses Antitrust Decision in Germany Over Data Collection. The New York Times.

Sava, R. (2020). Unwrapping the consent box. The CJEU Judgment in the Orange Romania Case.

Schermer, B.W. & Custers, B. and van der Hof, S. (2014). The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection, Ethics and Information Technology.

Seufert, E. (2023). What Is an "Appropriate Fee"? Mobile Dev Memo.

Solove, D. J, & Schwartz, P. M. (2021). EU Data Protection and the GPDR. Aspen Select Series, Wolters Kluwer, New York.

Solove, D. J. (2021). The Myth of the Privacy Paradox. George Washington Law Review 1.

Stoeklé, HC. (2017). Toward dynamic informed consent. Med Sci (Paris).

Tang, Jie, Akram, Umair, SHI, Wenjing. (2020). Why People Need Privacy? The Role of Privacy Fatigue in App Users' Intention to Disclose Privacy: Based on Personality Traits. Journal of Enterprise Information Management.

Testa, G., & Marelli, L. (2018). GDPR: rischi e opportunità del nuovo regolamento europeo per la protezione dei dati personali. Science, Università Statale di Milano e Istituto Europeo di Oncologia.

The Norwegian Consumer Council. (2022). Time to Ban Surveillance-Based Advertising.

Thobani, S. (2016). I requisiti del consenso al trattamento dei dati personali. Roma.

Usercentrics (2025). New Regulatory Updates for Cookie Use in Norway: What to Know and How to Comply.

Van den Bergh, R. (2021). The German Facebook Saga: Abuse of Dominance or Abuse of Competition Law? World Competition.

Vohs Kathleen, D. et al. (2008). Making Choices Impairs Subsequent Self-Control: A Limited-Resource Account of Decision Making, Self-Regulation, and Active Initiative. Journal of Personality and Social Psychology.

Volmar, M. N., & Helmdach, K. O. (2018). Protecting consumers and their data through competition law? Rethinking abuse of dominance in light of the Federal Cartel Office's Facebook investigation. European Competition Journal.

Weitzner, Daniel J. et al. (2008). Information Accountability. Communications of the ACM.

Wiedemann, K. (2020). The ECJ's Decision in "Planet49" (Case C-673/17): A Cookie Monster or Much Ado About Nothing? IIC - International Review of Intellectual Property and Competition Law.

Witt, A. C. (2021). Excessive data collection as a form of anticompetitive conduct – The German Facebook case. The Antitrust Bulletin.

World economic forum. (2013). Unlocking the Value of Personal Data: From Collection to Usage. Industry Agenda.

Yacoob, S. Y. (2024). Cookie Consent Requirements in Belgium.

Younas, A. & Bakhodir, T.o.M (2021). To What Extent are Consumers Harmed in the Digital Market from the Perspective of the GDPR? International Journal Of Multidisciplinary Research And Analysis.

Zeno-Zencovich, V. (2019). Do Data Markets Exist? Medialaws.

Zuboff, S., & Schwandt, K. (2019). The age of surveillance capitalism: the fight for a human future at the new frontier of power. Profile Books.

Legislation, acts and documents

Agencia Española de Protección de Datos, Guía sobre el uso de las cookies, 2024.

Article 29 Data Protection Working Party, Guidelines on consent under Regulation (EU) 2016/679, adopted on 28 November 2017, last revised and adopted on 10 April 2018, WP259 rev.01.

Article 29 Data Protection Working Party, WP29 Guidelines on Transparency under Regulation (EU) 2016/679, revised on 11 April 2018.

Article 29 Data Protection Working Party, Opinion 02/2013 on apps on smart devices, 27 February 2013.

Article 29 Data Protection Working Party, Opinion 04/2012 on the meaning of consent, 13 April 2012.

Article 29 Data Protection Working Party, The Future of Privacy – Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data, 1 December 2009, WP 168.

Article 29 Working Party, Opinion 04/2012 on cookie consent exemption (WP 194, 7 June 2012).

Article 29 Working Party, Working Document 02/2013 providing guidance on obtaining consent for cookies (WP 208, 2 October 2013).

Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, C 364/01, 18 December 2000.

Commission Nationale de l'Informatique et des Libertés, Cookie walls: la CNIL publie des premiers critères d'évaluation, 16 May 2022.

Datatilsynet, Brug af Cookie Walls, 20 February 2023.

Datenschutzkonferenz, Evaluation of Pur-Subscription Models on Websites, Resolution of the Conference of Independent Data Protection Supervisory Authorities of the Federal and State Governments, 22 March 2023.

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 as regards the better enforcement and modernisation of Union consumer protection rules, Official Journal of the European Union, L 328/7, 18 December 2019.

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, Official Journal of the European Union, L 136/1, 22 May 2019.

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 (Directive on privacy and electronic communications), Official Journal of the European Communities, L 201/37, 31 July 2002.

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC, 2002/65/EC and 2005/29/EC and Regulation (EC) No 2006/2004, Official Journal of the European Union, L 149/22, 11 June 2005.

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, Official Journal of the European Communities, L 281/31, 23 November 1995.

European Commission, 2017/0003 (COD), Proposal for a Regulation of the European Parliament and of the Council on the Protection of Personal Data in the Context of the Processing of Personal Data for Law Enforcement Purposes, COM/2017/010 final - 2017/03 (COD).

European Commission, Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act, Press Release IP/24/1689 of 25 March 2024.

European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 11 November 2010, COM (2010) 614 final.

European Data Protection Board, Annual Report 2024, published on April 2025.

European Data Protection Board, Position Paper on Interplay between Data Protection and Competition Law, adopted on 16 January 2025.

European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2020.

European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 4 April 2018.

European Data Protection Board, Letter on the European Commission's Cookie Pledge initiative, adopted on 13 December 2023.

European Data Protection Board, Opinion 08/2024 on valid consent in the context of consent or pay models implemented by large online platforms, 17 April 2024.

European Data Protection Board, Report of the work undertaken by the Cookie Banner Taskforce, 17 January 2023 (adoption).

European Data Protection Board, Statement on the review of the ePrivacy Directive and its impact on privacy and confidentiality in electronic communications, 25 May 2018.

European Data Protection Board, Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Article 66(2) GDPR), 27 October 2023.

European Data Protection Supervisor, Opinion 3/2015 (with addendum) – Europe's Big Opportunity: EDPS Recommendations on the EU's Options for Data Protection Reform, 27 July 2015.

European Parliament and Council, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal of the European Union, L 201/37, 31 July 2002.

European Parliament, Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Privacy and Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (e-Privacy Regulation), 20 October 2017, LIBE Committee, 2017/003COD, Amendment 24.

Italy, Legislative Decree No. 196/2003 of 30 June 2003 on the Protection of Personal Data (Privacy Code), as amended by Legislative Decree No. 101/2018, Official Journal of the Italian Republic, No. 174.

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, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, L 119/1, 4 May 2016.

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 (Digital Markets Act), Official Journal of the European Union, L 265/1, 12 October 2022.

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 (Digital Services Act), Official Journal of the European Union, L 277/1, 27 October 2022.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), Official Journal of the European Union, L 152/1, 3 June 2022.

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act), Official Journal of the European Union, L 2023/2854, 22 December 2023.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 establishing harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139, (EU) 2019/2144, and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828 (Artificial Intelligence Act), Official Journal of the European Union, L 1689/1, 12 July 2024.

Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Official Journal of the European Union, C 306/01, 17 December 2007.

Treaty on the Functioning of the European Union (TFEU), Official Journal of the European Union, C 326/47, 26 October 2012.

Relevant decisions

C-129/21, Proximus NV v. Gegevensbeschermingsautoriteit, Court of Justice of the European Union, judgment of 22 December 2022.

C-21/23, Lindenapotheke, Court of Justice of the European Union.

C-252/21, Meta Platforms, Court of Justice of the European Union.

C-61/19, Orange v. Romania, Court of Justice of the European Union.

C-673/17, Planet49, Court of Justice of the European Union.

C-97/23 P, WhatsApp Ireland, Advocate General Opinion, Court of Justice of the European Union.

T-136/23, Meta Platforms Ireland v European Data Protection Board, General Court (Tenth Chamber), Order of 29 April 2025.

European Union. (2024). Case T-319/24: Meta Platforms Ireland Ltd v European Data Protection Board, Action brought on 27 June 2024.

Italian Council of State (Section VI), Judgments No. 665 of 2021 and Nos. 7296 and 4357 of 2019.

Italian Council of State, Judgment No. 80 of January 7, 2025.

Italian Data Protection Authority, Provision No. 488.

Italian Data Protection Authority, Provision No. 488.

Italian Data Protection Authority, Decision of April 27, 2023.

Italian Data Protection Authority, Provision No. 389.

Italian Supreme Court, First Civil Section, judgment of 25 May 2021, No. 14381.

Italian Supreme Court, Judgment of January 29, 2016, no. 1748.

Italian Supreme Court, Order No. 28358 of 6 October 2023.

Österreichische Datenschutzbehörde, Case 2023-0.174.027, decided on 29 March 2023.

List of abbreviations

AG Advocate General

BEUC European Consumer Organisation

CJEU Court of Justice of the European Union

CNIL Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority)

CPC Consumer Protection Cooperation

CFR Charter of Fundamental Rights of the European Union

DCD Digital Content Directive

DPA Data Protection Authority

EDPB European Data Protection Board

EEA European Economic Area

EU European Union

GDPR General Data Protection Regulation

ICO Information Commissioner's Office (United Kingdom)

Meta Case Meta, Case C-252/21

NGO Non-Governmental Organization

NOYB None of Your Business (Digital Rights NGO)

WP29 Article 29 Data Protection Working Party

BKA Bundeskartellamt (German Competition Authority)

DMA Digital Markets Act

DSA Digital Services Act

DPC Data Protection Commission (Ireland)

EC European Commission

TFEU Treaty on the Functioning of the European Union