



FACULTY OF LAW

LUND UNIVERSITY

Salla Turunen

Subscribing for privacy: the validity of consent in "consent or pay" models under the General Data Protection Regulation

JAEM03 Master Thesis

European Business Law

30 higher education credits

Supervisor: Petra Gyöngyi

Term of graduation: Spring 2026

Table of contents

Summary	4
Preface.....	5
Abbreviations	6
1 INTRODUCTION	7
1.1 Background.....	7
1.2 Aim and research question	10
1.3 Delimitations	11
1.4 Methodology and material.....	11
1.5 Disposition.....	13
2 DEFINITION OF CONSENT WITHIN THE EU LEGAL FRAMEWORK.....	14
2.1 The General Data Protection Regulation.....	15
2.1.1 Definitions.....	16
2.1.2 The definition of consent: Article 4(11) GDPR.....	19
2.1.3 Consent as a legal base: Article 8(2) GDPR	20
2.1.4 Conditions for consent: Article 7 GDPR	21
2.1.5 Power imbalance: Recital 43 GDPR.....	22
2.2 The interpretation of the CJEU on consent	22
2.2.1 Active behaviour: no pre-ticked checkboxes	23
2.2.2 Informed consent.....	24
2.2.3 Freely given consent	25
2.2.4 Remarks.....	27
2.3 National Data Protection Authorities	28
2.4 EDPB interpretation of consent.....	29
3 CONSENT IN ‘CONSENT OR PAY’ MODELS	32
3.1 Closer look at consent or pay models.....	32
3.2 The oxymoron of consent within consent or pay models....	33
3.3 The building blocks of freely given consent	35
4 CRITICAL ANALYSIS OF FREELY GIVEN CONSENT IN LARGE ONLINE PLATFORMS: CASE STUDY ON META PLATFORMS	37
4.1 The technicalities of the subscription-based model.....	38
4.2 Assessment of consent obtained by Meta Platforms	39
4.2.1 Detriment to the data subject.....	39
4.2.2 Power imbalance between the controller and the data subject	42
4.2.3 Conditionality.....	43

4.2.4	Granularity	45
4.3	Deceptive design patterns in consent or pay models.....	46
4.4	Complementary GDPR principles.....	48
4.5	Counter argument: freedom to conduct business	50
5	CONCLUSION	53
6	Bibliography	55
6.1	EU Legislation.....	55
6.2	Scholarly Articles	55
6.3	Policy Papers	57
6.4	Online Sources.....	58
6.5	Books.....	61
6.6	Table Of Cases	61
6.7	Other Sources	62

Summary

This thesis analyses whether consent provided by data subjects as a legal basis for processing personal data for behavioural advertising in large online platforms is able to constitute valid, in particular freely given consent as it is understood under the GDPR.¹

The question has become significantly important as recent studies have indicated that majority of data subjects are choosing to consent² when faced with a consent or pay models, regardless of their actual willingness to data processing.³ The scrutiny around consent or pay models has developed into a well-discussed issue among the European Union regulators.⁴

¹ 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, repealing Directive 95/46/EC (General Data Protection Regulation) [2016] L 119/1, art 11.

² Timo Müller-Tribbensee, Klaus M. Miller, Bernd Skiera, 'Paying for Privacy: 'Paying for Privacy: Pay-or-Tracking Walls' (HEC Paris research paper No. MKG-2024-1514), p 37.

³ Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)informed Consent: Studying GDPR Consent Notices in the Field. (2019) ACM SIGSAC Conference on Computer and Communications Security, <<https://arxiv.org/pdf/1909.02638>> accessed 14 May 2026, p 10.

⁴ Patricia De Moraes, Paisane Matthey Claudet, 'Pay or consent to have your data used- the complex intersection between the DMA and data protection rules, International review of law, computers & technology (2026) University of East Anglia, p 2.

Preface

This thesis represents the conclusion of my studies at Lund University. I would like to express my gratitude to my supervisor Petra Gyöngyi who provided me with guidance during the writing of this thesis. I would also like to express gratitude to everyone who shared the past two years with me here in Lund.

Abbreviations

GDPR	European Data Protection Regulation
EU	European Union
EEA	European Economic Area
A29WP	Article 29 Working Party
EDPB	European Data Protection Board
DPA	Data Protection Authority
CNIL	Commission Nationale Informatique & Liberties
CJEU/ the Court	The Court of Justice of the European Union

1 INTRODUCTION

1.1 Background

The use of social media has been a defining feature of the 2000s. It has become an important tool for keeping in contact with one's inner circle and a way of finding new connections through mutual interests.⁵ Users of social media platforms, referred to as data subjects within the meaning of Article 4(1) GDPR⁶ are able to gain an access to these platforms by creating personal profiles,⁷ that are based on the information, (including full name, date of birth, gender and phone number) entered to the platform by the data subject themselves.⁸ This data is then merged together with the information collected on data subjects activities within and outside of the platform.⁹ Social media platforms that provide data subjects with free service by relying on the collection of such data have adopted a business model that generates its revenue by sharing personal data with third parties for advertising purposes.¹⁰

As a consequence of the development of internet and digital technologies, business models have experienced a change where the value of data has grown drastically and developed into a key source of revenue for companies operating in the online environment.¹¹ As stated by Meglena Kuneva, former European Consumer Commissioner in 2009, "*Personal data is the new oil of*

⁵ European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (13 April 2021), para 1<https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf> accessed 24 May 2026.

⁶ GDPR, art 4(1).

⁷ Guidelines 8/2020 (n5) para 19.

⁸ The difference between your Facebook account and profile (Facebook Help Center) <<https://www.facebook.com/help/327202558928776>>accessed 24 May 2026

⁹ EPDB Guidelines 8/2020 (n5) para 19.

¹⁰ Data policy (Instagram Help Center)< <https://help.instagram.com/155833707900388>>accessed 24 May 2026

¹¹ Luca Bolognini, Lorenzo Covello, Giuseppe Fiordalisi, 'Admissibility of the 'pay or consent' model: between digital economic revolution and data protection modernisation' (2024)< <https://zenodo.org/records/10848258> >accessed 30 March 2026

the internet and the new currency of the digital world”¹² The data collected by online platforms includes data subjects behavioural data, which is collected for several purposes, one of which is personalised advertising,¹³ which is essentially defined as advertisement tailored to data subjects based on behavioural and demographic data.¹⁴ The gathering and processing of data for the beforementioned purposes can be allowed through an express consent provided by data subject.¹⁵ In order for consent to be regarded as a lawful base for this kind of processing, it has to be informed, given voluntarily and the individual needs to have competence to make a decision.¹⁶

Following the years after the implementation of the GDPR, several online services started gradually adopting a new type of cookie wall, called ‘consent or pay’ or ‘pay or okay’, whereas the users of these online services were given two options: either consent to the processing on their personal data or paying to use the site.¹⁷ The model was first taken into use gradually by online newspapers, namely in Austria, Spain and Germany.¹⁸ In November 2023 Meta Inc, the owner of the biggest social media platforms, including Facebook and Instagram introduced the ‘consent or pay’ model to its users by offering two parallel models: a pay model and an advertising-funded model¹⁹ The data subjects in the EU that were using these platforms were given a choice between subscribing to a monthly fee without personalised advertising or to

¹² World Economic Forum, Personal Data: The Emergence of a New Asset Class (2011) <https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf> accessed 20 April 2026

¹³ Sangjun Nam, Youngsun Kwon, ‘Is pay-or-consent for privacy justifiable? Evidence from different users’ privacy attitudes toward behavioral data collection in South Korea’ School of Business and Technology Management, Telecommunications policy (2024).

¹⁴ Morimoto, M. (2021). Privacy concerns about personalized advertising across multiple social media platforms in Japan: the relationship with information control and persuasion knowledge. *International Journal of Advertising*, 40(3), p 431–451.

¹⁵ Daniel J Solove, Murky consent: an approach to the fictions of consent in privacy law, *Harvard Law Review* 1880 (2013) p 569.

¹⁶ Emma C. Bullock, Valid Consent, *The routledge handbook of the ethics of consent* (2018) p 85-86.

¹⁷ Datatilsynet ‘Request for an EDPB opinion on “consent or pay” (Datatilsynet) <<https://www.datatilsynet.no/en/news/aktuelle-nyheter-2024/request-for-an-edpb-opinion-on-consent-or-pay/>> accessed 25 February 2026.

¹⁸ Noyb, Pay or Okay Report (2025) <https://noyb.eu/sites/default/files/2025-07/Pay_or_Okay_Report_2025_web.pdf> accessed 24 May 2026

¹⁹ Prof Dr Martin Nettesheim EU Data Protection Law and Pay-or-Consent Business Models, University of Tübingen Law School (2024) p 2. <<https://dx.doi.org/10.2139/ssrn.4768419>> accessed 24 May 2026

keep using the platform and through that accept that the use of personal data for various purposes, including personalised advertising.²⁰

The ‘consent or pay’ model, implemented by Meta results in the application of both the GDPR and ePrivacy Directive.²¹ The GDPR establishes the rules on the processing of the personal data while the ePrivacy Directive, supplementing the GDPR, sets out additional rules concerning the use of technologies related to tracking, including cookies.²² The interplay of the two was clarified by the CJEU in a case *Planet49*²³, which ruled that Article 5(3) of ePrivacy Directive, read in conjunction with Article 4(11) and Article 6(1)(a) GDPR requires consent to be active positive action in order to be valid.²⁴ This is because according to ePrivacy directive, data subject needs to give consent to cookies, whereas consent is defined in GDPR 4(11) and interpreted as active behaviour.²⁵

Nevertheless, according to a recent study published in a HEC Paris research paper, 99% of users choose to consent to tracking when they are faced with pay or consent walls.²⁶ The results are consistent with a study from 2019, which declared that only around 3% of users are voluntarily accepting marketing cookies.²⁷ This raises the question of whether consent or pay models are capable of providing data subjects with a free choice that is in accordance with the requirements of the GDPR. It also raises a concern whether data sub-

²⁰European Commission, Commission sends preliminary findings to Meta over its “Pay or Consent” model for breach of the Digital Markets Act (2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3582> accessed 24 May 2026.

²¹ Alessia D’Amico, Dionysios Pelekis, Cristiana Santos, and Bram Duivenvoorde, *Meta’s Pay-or-Okay Model, An analysis under EU Data Protection, Consumer and Competition Law, Technology and Regulation* (2024), p 257.

²² D’Amico,(n21)p 257.

²³ Case C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH ECLI:EU:C:2019:801.

²⁴ Planet49 (n 23) para 49-52.

²⁵ Planet49 (n 23) para 49-52.

²⁶ Müller-Tribbensee (n2) p 37.

²⁷ Utz (n3), p10.

jects are actually agreeing to data processing or whether such consent is influenced by factors including the user's desire to continue using the service free of cost and lack of equivalent lack of alternatives.²⁸

1.2 Aim and research question

The purpose of this thesis is to examine the validity of consent in 'consent or pay' models implemented by online platforms within the EEA from the perspective of the GDPR. The thesis assesses whether data subjects can exercise valid, freely given consent as it is set out in the GDPR, when confronted with consent or pay models.

To address the forementioned objective the main research question can be formulated as follows: To what extent is the 'consent or pay' model implemented by large online platforms compatible with the requirement of freely given consent under article 4(11) GDPR?

To be able to answer the main research question, the three following research questions will be used, formulated as follows:

1. How is valid consent understood under the GDPR and how has the concept been interpreted and developed through CJEU case law and EDPB recommendations?
2. To what extent are data subjects able to exercise a valid, in particular freely given consent, when faced with a consent or pay model implemented in large online platforms and what are the conditions these platforms have to meet in order to fulfil the requirement of freely given consent?

²⁸ EDPB Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, (17 April 2024) para 105. <https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf> accessed 24 May 2026.

3. To what extent does the consent or pay model implemented by Meta platforms fulfil the requirement of freely given consent as it is understood in GDPR?

1.3 Delimitations

The scope of this thesis is limited to the analysis of consent under the GDPR, the interpretations and clarifications of the CJEU and policy documents published by EDPB and other data protection authorities from the Member States. While acknowledging the interplay between GDPR and ePrivacy Directive, the thesis does not include the ePrivacy Directive for further analysis to guarantee a narrow research focus. While the Digital Markets Act (DMA) is acknowledged as complementary to the GDPR and the non-compliance decision by the European Commission on Meta's consent or pay model for the breach of DMA is deemed as important, it has been deliberately left out from the deeper analysis to maintain the focus on one framework: the GDPR.

The geographical scope of the thesis is limited to the European Union. In terms of Meta Platforms, the focus of this thesis is on the consent or pay model implemented in EU, EEA and Switzerland.

1.4 Methodology and material

The thesis follows a doctrinal legal method that analyses the concept of consent from the viewpoint of the General Data Protection Regulation²⁹, the legal framework regulating consent for the processing of personal data in the European Economic Area, the interpretation of the Court of Justice of the European Union and guidance provided by European Data Protection Board. The thesis identifies the criterion of valid, in particular freely given consent and

²⁹ GDPR (n1).

examines whether consent or pay models implemented by large online platforms are able to provide data subjects with an opportunity to exercise consent that fulfils this criterion.

Doctrinal legal research method is chosen as appropriate as it aims to create a presentation of the principles and rules that govern a certain legal field and analyse the relationship between those principles while clarifying gaps and uncertainties in the existing law.³⁰ By applying doctrinal research method, the first part of the thesis analyses the meaning behind the definition of “consent” set out in Article 4(11) of the GDPR. The research aims to analyse the relationship between the law, the interpretation of the CJEU and the opinions and recommendations of the data protection authorities to create a coherent understanding on the concept of consent under the EU legal framework. The second part of the thesis applies the understanding developed in the first part to assess whether the consent or pay models implemented by large online platforms are able to provide data subjects with an opportunity to exercise valid consent as it is defined in the first part of this thesis.

The research relies upon close reading of primary legal sources, particularly the General Data Protection Regulation and EU Charter of Fundamental Rights. The aforementioned sources are complemented by selected case law from the Court of Justice of the European Union, as well as policy documents from the European Data Protection Board and publications of National Data Protection Authorities from selected Member States. The analysis is supplemented by secondary sources, including academic commentary and textbooks on GDPR as well as recent reports published by NOYB. The sources are selected due to their relevance to the subject matter of this thesis.

³⁰ Jan M Smiths, ‘What is legal doctrine? on the aims and methods of legal-dogmatic research, Maastricht European private law institute working paper no. 2015/06, p 5.

1.5 Disposition

The thesis is divided into five chapters. Following the introductory chapter, the second chapter delves into the concept of consent by providing an overview on how consent is defined in the GDPR. This definition is developed through analysis of CJEU case law and EDPB guidance as well as data protection authorities' publications.

Building on this foundation, the third chapter moves on to examining consent in consent or pay models. For the first part, the chapter examines whether data subjects are actually able to grasp what is it, that they are consenting to in relation to recent studies conducted on related matters. The second part of the chapter outlines the criteria of freely given consent, outlined by the EDPB, keeping in mind the concept of consent developed in the second chapter.

The fourth chapter reflects the concept of consent assessed in the second chapter to the set of criteria developed in the third chapter and creates a case study on Meta Platforms. The main aim of the chapter is to examine whether very large online platforms with dominant market position implementing subscription- based consent or pay models can provide data subjects with a choice that constitutes a valid, freely given consent as stipulated under the GDPR.

Finally, chapter five concludes the thesis by summarizing the main findings.

2 DEFINITION OF CONSENT WITHIN THE EU LEGAL FRAMEWORK

The protection of natural persons in the context of the processing of personal data is a fundamental right³¹, enriched in Article 8 of the EU Charter of Fundamental Rights³² and Article 16 of the Treaty on the Functioning of the European Union.³³ These rights are enforced by the General Data Protection Regulation (hereinafter referred to as GDPR) which entered into force in 2016 and became fully applicable in 2018. It establishes obligations for organizations that collect or process data related to people in the EU³⁴ with the objective of ensuring that natural persons receive high level of protection in relation to the processing of personal data in all Member States of the Union while minimising obstacles in the flow of personal data within the European Union.³⁵ The principles relating to processing of personal data are found from Article 5 GDPR.³⁶ As set forth in Article 5(1)(a), “*personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*”.³⁷ Whereas the lawfulness of processing of personal data is anchored in six legal grounds,³⁸ enshrined in Article 6 GDPR.³⁹

This chapter examines how the concept of consent is perceived within the EU legal order from the perspective of the GDPR, the Court of Justice of the European Union (hereinafter referred to as the CJEU) case law, the publications of the European Data Protection Board (hereinafter referred to as the EDPB)

³¹ GDPR (n1) Recital 1.

³² EU Charter of Fundamental Rights, art 8.

³³ Treaty on the Functioning of the European Union, art 16.

³⁴ What is GDPR, the EU’s new data protection law? <<https://gdpr.eu/what-is-gdpr/>> accessed 3 March 2026.

³⁵ GDPR (n1) Recital 10.

³⁶ GDPR (n1) Article 5.

³⁷ GDPR (n1) Article 5(1).

³⁸ Article 29 data protection working party, Opinion 15/2011 on the definition of consent (13 July 2011) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> accessed 24 May 2026

³⁹ GDPR (n1) Article 6(1).

and the guidelines and opinions of the National Data Protection Authorities of the selected Member States.

2.1 The General Data Protection Regulation

The GDPR is one of the most substantive pieces of legislation on data protection.⁴⁰ The protection of individuals in relation to their personal data lies at the core of GDPR.⁴¹ It elaborates previous legislation on data protection (Directive 95/46/EC and Directive 2002/58/EC) while adding new rights and obligations as well as developing better protection for data subjects.⁴² The GDPR has a dual-purpose objective, which aims to protect the fundamental rights and freedoms of data subjects while at the same time enabling the free movement of personal data within the European Union.⁴³ The protection of fundamental rights in relation to data processing, as stipulated in Recital 1 of the GDPR⁴⁴ strives to equip data subjects with a certain level of sovereignty that translates into a control over ones' personal data.⁴⁵

According to the GDPR that personal data can be processed only when certain legal bases and principles related to data protection are fulfilled.⁴⁶ The principles, stipulated as the following are closely linked to each other: lawfulness, fairness, transparency, purpose limitation, data minimisation, accountability, integrity and confidentiality, storage limitation and accuracy.⁴⁷ Principles of data minimisation and purpose limitation, stipulated in Article 5 GDPR enhance the protection data subjects by providing limits to data processing.⁴⁸ Services used by data subjects have to be created in line with principles of⁴⁹

⁴⁰What is GDPR, The EU's new data protection law?' <<https://gdpr.eu/what-is-gdpr/>> accessed 3 March 2026.

⁴¹ De Moraes (n4) p4.

⁴²Forbrukerrådet, DECEIVED BY DESIGN, How tech companies use dark patterns to discourage us from exercising our rights to privacy (2018)<<https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf>> accessed 18 April 2026

⁴³ GDPR (n1), Article 1.

⁴⁴ GDPR (n1) Recital 1.

⁴⁵ De Moraes (n4), p4.

⁴⁶ Forbrukerrådet (n42)

⁴⁷ Denis Kelleher, Kare.n Murray, EU Data protection law, Bloomsbury (2018) p 137.

⁴⁸ GDPR (n1) Article 5 .

⁴⁹Forbrukerrådet (n42).

data protection by design, which entails the obligation of services to guarantee that principles related to data processing are adhered to and data protection by default, which aims to ensure that personal data of data subjects is inherently protected.⁵⁰

The GDPR addresses consent on several provisions, particularly in articles 4(11), 6(1)(a), 7 and applicable recital 43. With regard to consent, the GDPR has further specified the requirements of acquiring and demonstrating valid consent from how it was defined in the earlier forms of data protection legislation, namely Data Protection Directive.⁵¹

2.1.1 Definitions

This section provides definitions of the key GDPR terms used throughout this thesis for the purpose of ensuring a comprehensive understanding of the topic discussed.

Personal data means “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.⁵² The definition of personal data has stayed relatively unchanged from Directive 95/46/EC, with minor differences⁵³, related to technologies that were less developed when the Directive was formulated.⁵⁴ The CJEU has further evaluated the

⁵⁰ GDPR (n1) Article 25.

⁵¹ EDPB Guidelines 05/2020 on consent under Regulation 2016/679 (4 May 2020) <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 24 May 2026.

⁵² GDPR (n1) Article 4(1)

⁵³ Kelleher (n47) p80..

⁵⁴ Rosemary Jay, Guide to the General Data Protection Regulation, A companion to Data Protection Law Practise (4th edition) (2017), p 54.

definition of personal data to include⁵⁵ tax data related to income⁵⁶, fingerprints⁵⁷, photograph of an individual⁵⁸, marital status, place of birth and nationality.⁵⁹

Processing means “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.⁶⁰ The definition has remained largely unchanged from the preceding directive, by incorporating “sets of personal data” to the definition. The slight adjustments in the definition arise from new types of processing operations, which had been developed after the drafting of the earlier directive.⁶¹

Consent means “any freely given, specific, informed and unambiguous indication of the data subject’s wish by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”⁶² The earlier version of the term consent in the preceding directive did not include the word “unambiguous” in its definition, but instead included it in a separate article, providing further requirements of consent that should be read together with the definition provided in the definitions section.⁶³ Additionally, the definition set out in the GDPR included “personal data relating to him or her” instead of the earlier version of “personal data relating to him”.⁶⁴

⁵⁵ Kelleher (n47) p 80.

⁵⁶ Case-201/14 Bara and Others, para 15.

⁵⁷ Case-291/12 Michael Schwartz v Stadt Bochum, para 27

⁵⁸ Case-212/13 František Ryneš V Úřad pro ochranu osobních údajů, ECLI:EU:C:2014:2428, para 22.

⁵⁹ Case-524/06 Huber, ECLI:EU:C:2008:724 para 31, 43, 43.

⁶⁰ GDPR (n1) Article 4(2).

⁶¹ Rosemary (n54), p55.

⁶² GDPR (n1) Article 4 (11).

⁶³ A29WP (n38) p 21.

⁶⁴ 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, OJ L 281, Article 2(h).

Controller means “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law”.⁶⁵ The definition has stayed relatively unchanged from Directive 95/46 with minor adjustments. The CJEU has interpreted the definition in several cases⁶⁶ including *Google Spain*⁶⁷ and *Manni*.⁶⁸ The EDPB has provided guidance by explaining that controller is a body that establishes the purposes and means of processing.⁶⁹ It ascertains that besides being defined by law, controllership can be included in some roles, such as employer.⁷⁰

Processor means “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.”⁷¹ The definition provided in Directive 95/46/EC⁷² has withstood the passage of time by staying precisely the same throughout the development of GDPR. The EDPB provides guidance by explaining that processor has to be a separate entity in relation to the controller and the processing of personal data on the behalf of the controller.⁷³

Meanwhile the term processing is set out in Article 4(2) GDPR, *tracking* is a much narrower concept, covered by article 5(3) ePrivacy Directive⁷⁴, which

⁶⁵ GDPR (n1) Article 4 (7).

⁶⁶ Kelleher (n47) p 98.

⁶⁷ Case-131/12 Costeja Gonzalez v Google Spain and Google, ECLI:EU:C:2014:317, para 33.

⁶⁸ Case-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce V Salvatore Manni, ECLI:EU:C:2017:197, para 35.

⁶⁹ EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, (7 July 2021), p 3 <https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf> accessed 24 May 2026

⁷⁰ Guidelines 07/2020 (n69) p 3.

⁷¹ GDPR (n1) Article 4 (8).

⁷² Data Protection Directive (n64) Article 2 (e)

⁷³ EDPB Guidelines 07/2020 (n68), p 3.

⁷⁴ 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) (2002) OJ L 201 Article 5(3).

governs the use of technologies related to tracking.⁷⁵ It states that “Member States shall ensure that the use of electronic communications networks to store information is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller.”⁷⁶

Lastly, *Cookie walls* are defined as banners, which typically appear at the point of accessing a website. Typically, cookie walls provide data subjects with a choice between consenting to the processing of personal data which enables them to access the website or declining consent which often means no access to the service.⁷⁷ Cookie walls are not explicitly defined under GDPR nor the ePrivacy Directive. The guidance of the EDPB has provided that cookie walls cannot constitute a valid, freely given consent.⁷⁸

2.1.2 The definition of consent: Article 4(11) GDPR

Traditionally, consent has been regarded as lying at the core of data protection.⁷⁹ The underlying idea behind consent is to provide individuals with the right to ascertain under what circumstances, how and to what extent can information about them be used and for what purposes.⁸⁰ Article 4(11) GDPR requires consent to be *freely given, specific, informed and unambiguous*.⁸¹ The A29WP has pointed out that the condition of “*freely given*”, elaborated more in Article 7(4) and recital 42 GDPR,⁸² provides that there should be a real choice and control practised by data subjects when it comes to consenting

⁷⁵ ePrivacy Directive (n74).

⁷⁶ ePrivacy Directive (n74) Article 5(3).

⁷⁷ EDPB Guidelines 05/2020 (n51) p 16.

⁷⁸ EDPB Guidelines 05/2020 (n51), para 39.

⁷⁹ Eleni Kosta, Ronald Leenes, Research Handbook on EU data protection law 2021: Bart Custers, Eduard Fosch-Villaronga, Simone Vander Hof, Bart Schermer, Alan M. Sears and Aurelia Tamo-Larrieux, The role of consent in an algorithmic society-its evolution, scope, failings, and re-conceptualization, p 457-458.

⁸⁰ Kosta In79) p 455.

⁸¹ GDPR (n1) Article 4(11).

⁸² D’Amico (n21) p 257.

to data processing operations.⁸³ Consent should be given by a clear affirmative act that establishes that the data subject has agreed to the processing of personal data concerning her or him.⁸⁴ The affirmative act establishing the consent should be unambiguous, but it can take many forms, including written form, oral statement or electronic means.⁸⁵ In practice, it could mean choosing to tick a box while visiting a website with a banner asking for consent.⁸⁶ In order for a data subject to give informed consent, they should be made aware of the identity of the controller as well as the purposes for which the processing of their personal data are related to.⁸⁷

2.1.3 Consent as a legal base: Article 8(2) GDPR

First and foremost, it should be mentioned that the core assumption behind consent as a legal base appears to be that data subjects are able to make logical, independent and self-aware decisions regarding the processing of their personal data.⁸⁸ The actual competence of data subjects to make these decisions is subject to scholarly debate.⁸⁹ Some scholarly articles argue that there is a gap between the legal theory that rests on the assumption that data subjects make deliberate decisions and the real life where data subjects are likely to just consent blindly without reading the terms.⁹⁰

Article 8(2) of the Charter provides that personal data must be processed “on the basis of the consent of the person concerned or some other legitimate basis laid down by law.”⁹¹ Article 6 of the GDPR⁹² gives effect to Article 8(2) of the Charter by establishing six legal bases for the processing of personal data.

⁸³ Article 29 Working Party Guidelines on consent under Regulation 2016/679 (28 November 2017), p 5.

⁸⁴ GDPR (n1) recital 32.

⁸⁵ GDPR (n1) recital 32.

⁸⁶ GDPR (n1) recital 32.

⁸⁷ GDPR (n1) recital 42.

⁸⁸ Dr. Bart W. Schermer, dr. Bart Custers, prof. Simone van der Hof, ‘The Crisis of Consent, How Stronger Legal Protection may lead to Weaker Consent in Data Protection’, Leiden University Faculty of Law, *Ethics and Information Technology* (2014), p 1.

⁸⁹ Schermer (n88).

⁹⁰ Custers (n 88) p2.

⁹¹ EU Charter (n32) Article 8(2).

⁹² GDPR (n1) Article 6 (1).

The legal grounds are consent, performance of a contract, compliance with a legal obligation, protection of vital interests, public interest or exercise of official authority and legitimate interests.⁹³ In order for the processing to be considered lawful, one or more legal bases has to be applied.⁹⁴ As established in Article 6(1)(a), the consent of the data subject is one of the six legal grounds. Consent as a legal base, states that processing of data shall be lawful if the *data subject has given consent to the processing of his or her personal data for one of more specific purposes*.⁹⁵ The controller bears the responsibility of choosing the appropriate basis that justifies the processing of personal data. Consent as a justification is lawful only when the data subject is offered a choice that satisfies the conditions⁹⁶ set out in Article 7 of the GDPR.⁹⁷

2.1.4 Conditions for consent: Article 7 GDPR

The conditions for consent are enriched in article 7 GDPR.⁹⁸ Article 7(1)⁹⁹ sets forth that the burden of proof in whether a data subject consented to processing to his or her personal data is onto the controller.¹⁰⁰ The subsection 7(2) stipulates that consent in the form of written declaration that also concerns other matters must be presented clearly separated from the other issues, in a form that's easily accessible and in plain and clear language.¹⁰¹ Subsection 7(3) grants the data subject the right to withdraw his or her consent at any time.¹⁰² Subsection 7(4) states that when assessing whether consent is freely given, it should be considered whether the performance of a contract is conditional on consent,¹⁰³ meaning that consent has been given as an exchange

⁹³ GDPR (n1) Article 6(1).

⁹⁴ Amar Tauqeer, An integrated approach to GDPR-compliant data sharing employing consent, contracts, and licenses, *Data & Knowledge Engineering*, volume 162 (2026).

⁹⁵ GDPR (n1) Article 6(1)(a).

⁹⁶ EPDB Guidelines 05/2020 (n51), p5.

⁹⁷ GDPR (n1) Article 7.

⁹⁸ GDPR (n1) Article 7. .

⁹⁹ GDPR (n1) Article 7(1).

¹⁰⁰ Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *The EU General Data Protection Regulation (GDPR) A commentary*, Oxford University press (2020), p 18.

¹⁰¹ GDPR (n1) Article 7(2).

¹⁰² GDPR (n1) Article 7(3).

¹⁰³ GDPR (n1) Article 7(4).

for a service.¹⁰⁴ The meaning behind the subsection 7(4) has been a subject of scrutiny as there is no one consensus on whether personal data can be monetized as something given in exchange.¹⁰⁵ Some scholars argue for the monetization of personal data whereas others do not accept the idea.¹⁰⁶ For instance, article 29WP provides that consent must not be a counter performance of a contract,¹⁰⁷ unless there is a genuine choice offered to the data subject.¹⁰⁸ Therefore, it could be argued that personal data can be monetized if it is a result of genuine will of the data subject and there is no conditionality without an equivalent alternative present.¹⁰⁹

2.1.5 Power imbalance: Recital 43 GDPR

Recital 43¹¹⁰ delimits the interpretation of free consent by stating two things. Firstly, when the controller and the data subject have an imbalance in power between them, the appropriate legal bases for the processing of personal data should be something else than consent. This applies specifically in situations where the controller is a public authority,¹¹¹ as in these situations the data subject cannot be regarded as having other realistic options, than accepting the processing,¹¹² meaning that the consent could not be considered as truly freely given.¹¹³ Another factor delimiting the interpretation of free consent is that, in situations where the performance of a contract is dependent on consent, even though consent is not needed for the performance should be presumed as not to be freely given.¹¹⁴

2.2 The interpretation of the CJEU on consent

¹⁰⁴ Václav Janeček, Gianclaudio Malgieri, 'Commerce in Data and the Dynamically Limited Alienability Rule', Cambridge University press (2019),p 931.

¹⁰⁵ Janeček (n104)

¹⁰⁶ Janeček (n104) p 931.

¹⁰⁷ A29WP Guidelines 2016/679 (n83) p 8.

¹⁰⁸ A29WP Guidelines 2016/679 (n83), p 9.

Janeček(n104) p 932.

¹¹⁰ GDPR (n1) Recital 43.

¹¹¹ GDPR (n1) Recital 43.

¹¹² A29WP Guidelines 2016/679 (n83) p 6.

¹¹³ GDPR (n1) Recital 43

¹¹⁴ GDPR (n1) Recital 43.

Next, it is necessary to analyse how the CJEU has interpreted consent in case law. While the GDPR doesn't tackle issues related to processors market position,¹¹⁵ or the business model of the processor,¹¹⁶ and therefore doesn't assess how these aspects can influence the validity of data subjects expressed consent for the processing of personal data.¹¹⁷ The first two cases selected for this chapter demonstrate the requirements of valid consent under GDPR in practise, meanwhile the third case reflects freely given consent together with issues traditionally governed under the DMA, including market power.¹¹⁸

2.2.1 Active behaviour: no pre-ticked checkboxes

In *Bundesverband der Verbraucherzentralen und Verbraucherverbände V Planet49 GmbH*¹¹⁹ (hereinafter referred to as *Planet49*) the Court clarified the concept of “unambiguous consent” to mean that the indication given by the data subject to consent to processing of personal data must be based on active behaviour.¹²⁰ The case concerned an online lottery, coordinated by Planet49 where everyone who wanted to register for the lottery had to deselect a pre-ticked checkbox that authorised the installation of cookies.¹²¹ The court ruled that pre-ticked checkbox, which data subjects have to deselect in order to refuse to consent do now constitute a valid consent under GDPR regime.¹²² This is because a pre-ticked checkbox makes it difficult to determine whether the data subject had actually read or noticed the checkbox and decided to keep it ticked as a confirmation of consent.¹²³ The court also clarified

¹¹⁵ D' Amico (n21).

¹¹⁶ De Moraes (n4) p4.

¹¹⁷ De Moraes (n4) p4.

¹¹⁸ De Moraes (n4) p 1.

¹¹⁹ Planet49 (n23).

¹²⁰ Planet49 (n23).

¹²¹ Planet49 (n2).

¹²² Planet49 (n23) para 63

¹²³ Planet 49(n23) para 55.

that service providers are required to provide data subjects information regarding the length of the operation of cookies and whether third parties have also gained an access to them.¹²⁴

2.2.2 Informed consent

In *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*¹²⁵ the CJEU affirmed the principle established earlier by the Planet49 judgment and specified another important element in relation to consent: informed consent.¹²⁶ The case concerned a situation where Orange Romania, a mobile telecommunications service provider had preserved copies of the identity documents of its customers without showcasing that the customers had given their valid consent for the storing activities.¹²⁷ The customers of Orange Romania had been offered a contract for telecommunication services, that had included a clause with a pre-ticked box, confirming that the data subject is informed and consents that there will be a copy of her identify document that will be collected and stored for identification purposes.¹²⁸ Customer, who did not grant a permission for the storing of their personal data were required to state this in a writing,¹²⁹ creating a situation, where refusing to consent constitutes an active behaviour, whereas consenting is passive, as noted by the Advocate General.¹³⁰ The issue in hand was that the customers were not informed, whether the refusal to consenting would lead to not concluding the contract, meaning that the customers did not know the possible consequences resulting from their decision.¹³¹

¹²⁴ Planet49 (n23).

¹²⁵ Case-61/19, *Orange România SA V Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* ECLI:EU:C:2020:901.

¹²⁶ *Orange Romania* (n125) para 37.

¹²⁷ *Orange Romania* (n125) para 21.

¹²⁸ *Orange Romania* (n125) para 53.

¹²⁹ *Orange Romania* (n125) para 50.

¹³⁰ Case-61/19, *Orange România SA V Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* Opinion of Advocate general, ECLI:EU:C:2020:158 para 60.

¹³¹ Opinion of AG, *Orange Romania* (n130)

Therefore, the Court clarified the concept of informed consent in practise, by interpreting the meaning of informed under Article 4(11) GDPR.¹³²

2.2.3 Freely given consent

In a consequential case *Meta Platforms Inc and Others v Bundeskartellamt*¹³³ the Court clarified whether the dominant market position of Meta Platforms prevents data subjects from exercising valid consent under GDPR.¹³⁴ By analysing this, the Court determined the relationship between competition law and GDPR.¹³⁵ The case was about Meta Platforms Ireland, which runs Facebook that operates in the European Union region. The case concerned the nature of the business model, applied by Facebook, which was built on generating revenue through online advertising that is based on characteristics of the data subjects, including online behaviour, personal interests and individual circumstances.¹³⁶ In 2019 Bundeskartellamt, a German competition authority¹³⁷ brought proceedings against Meta Platforms and issued a decision stating that Facebook is abusing its dominant position in the social network market¹³⁸ by requiring data subjects in Germany to consent to the collection of personal data as a prerequisite for using Facebook.¹³⁹ During the same year, Meta Platforms challenged the decision¹⁴⁰ and updated the general terms of Meta Platforms Ireland, expressing it to the data subjects that they are agreeing to being shown advertisements instead of having to pay for using Facebooks services.¹⁴¹ The Higher Regional Court of Düsseldorf decided to stay

¹³² GDPR (n1) Article 4(11).

¹³³ Case C-252/21 Facebook Deutschland GmbH v Bundeskartellamt, ECLI:EU:C:2023:537

¹³⁴ Bundeskartellamt (n133) para 155(8)

¹³⁵ Peter J. van de Waerdt, *Meta v Bundeskartellamt: Something Old, Something New*, European Papers, Vol 8, 2023, No 3, PP. 1077-1103.

¹³⁶ Bundeskartellamt (n133) para 27

¹³⁷ Bundeskartellamt official website <<https://www.bundeskartellamt.de/EN/Bundeskartellamt/AboutUs/aboutus.html#:~:text=The%20Bundeskartellamt%20is%20the%20most,to%20protect%20competition%20in%20Germany>> Accessed 24 May 2026.

¹³⁸ Bundeskartellamt case summary, Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing, case Summary (February 2019,) B6-22/16, p 7.

¹³⁹ Bundeskartellamt case summary(n138) p1.

¹⁴⁰ Bundeskartellamt (n133) para 31.

¹⁴¹ Bundeskartellamt (n133) para 32

the proceedings and instead refer questions for the preliminary ruling of the Court of Justice.¹⁴² The questions referred included a question on whether the users of online services, such as Meta Platforms Ireland, that have a dominant market position, are able to consent to the processing to their personal data as required under GDPR Articles 4(11), 6(1)(a) and 9(2)(a).¹⁴³ The Court built its arguments from the content of recitals 42 and 43 and Article 7(4) of GDPR, which expressed the conditions of freely given consent, that include a genuine choice, ability to withdraw, lack of imbalance between controller and data subject and separate consent for each operation concerning the processing of personal data as well as whether the performance of a contract is dependent on the consent to processing of personal data that is not necessary for carrying out the contract.¹⁴⁴

The Court examined that a dominant position on the market held by an online social network does not by default prevent the data subjects of that online social network from being able to exercise consent within the meaning of article 4(11) GDPR.¹⁴⁵ However it noted that a dominant market position is an element that should be taken into consideration when conducting an assessment on whether there is the consent given fulfils the criteria of valid consent, as the setting is prone to have an influence on freedom of choice of the data subjects.¹⁴⁶ The court also noted that in accordance with recital 7(4) of the GDPR, dominant position on the market can create an imbalance between the data subject and the controller, which can lean towards enforcing conditions that are not essential for the performance of the contract,¹⁴⁷ which would be on the contrary to the requirements of lawful processing, as stipulated in Article 6 (1)(b) of GDPR.¹⁴⁸

The Court then clarified that data subjects have the right to decline data processing operations that are not necessary for conducting the contract while

¹⁴² Bundeskartellamt (n133) para 35.

¹⁴³ Bundeskartellamt (n133) para 35(6).

¹⁴⁴ Bundeskartellamt (n133) para 143–145.

¹⁴⁵ Bundeskartellamt (n133), para 155.

¹⁴⁶ Bundeskartellamt (n133), para 148.

¹⁴⁷ Bundeskartellamt (n133) para 149.

¹⁴⁸ GDPR (n1)Article 6(1)(b).

still being able to access the online service in question. If needed, these users could be offered a fee as an alternative option to consenting to data processing. The court described the fee as “appropriate” and as “an equivalent alternative.”¹⁴⁹ However, the definition of what kind of amount would qualify these criteria was not specified further. According to Noyb, an appropriate fee could have for example the following elements: the price would not have a significant impact on whether data subjects decide to consent or not and a price similar to the profit made from personalized advertisement.¹⁵⁰

2.2.4 Remarks

Taken together, the case law, particularly in rulings of *Orange Romania* and *Planet49* demonstrates how legitimate consent requires that data subject holds enough information regarding the processing operations related to his or her data how consent has to consist of active behaviour on the behalf of the data subject, denying the use of pre-checked checkboxes that assume consent as a default. The rulings also showcase how the CJEU interprets the concept of valid consent in a rigorous manner, in conformity with the A29WP and EDPB guidelines.¹⁵¹

Meta Platforms Inc and Others v Bundeskartellamt is regarded as a landmark case that reflects the relationship between the competition law and data protection. In terms of freely given consent, the ruling considered how power imbalance, detriment to the data subject, granularity and conditionality can affect whether condition can be deemed as valid under the GDPR. After the ruling, the scrutiny around consent or pay models that rely on the consent of the data subject as an exchange for the free use of service heightened and developed into a well-discussed issue among the European Union regulators.¹⁵²

¹⁴⁹ Bundeskartellamt (n133) Para 150.

¹⁵⁰ Noyb, ‘Complaint under article 77(1) GDPR’ (November 2023) p 9.
<<https://noyb.eu/sites/default/files/2023-11/Complaint%20-%20Meta%20Pay%20or%20Okay%20-%20REDACTED.pdf>> accessed 24 May 2026

¹⁵¹ Kuner (n100), p 47.

¹⁵² De Moraes (n4) p 2.

2.3 National Data Protection Authorities

Each country in the European Economic Area (EEA) has their own national data protection authority (DPA) appointed. The rights and obligations of the national data protection authorities are enriched in article 58 GDPR.¹⁵³ Broadly speaking, the role of DPA is to supervise and implement the application of the GDPR within a Member State.¹⁵⁴ They provide citizens and companies with information on their rights and obligations¹⁵⁵ and give guidance to national institutions, including government on data protection matters.¹⁵⁶

During the years of 2019-2020, scrutiny around the topic of cookies and tracking techniques started to increase and various national data protection authorities concerned on the matter published documents addressing the issue, including France, Spain and Germany.¹⁵⁷ In 2019, the French data protection authority ‘CNIL’ took a stance on online advertising rules and published guidelines¹⁵⁸ regarding cookies and other trackers. The guidelines also touched upon the concept of consent, highlighting the importance of valid expression as a requirement of consent. The guidelines provided that valid expression of consent cannot be deducted from the fact that the data subject

¹⁵³ GDPR (n1) Article 58.

¹⁵⁴ An Official Website of the European Union, Data protection authority & you <https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-authority-and-you_en>accessed 27 March 2026.

¹⁵⁵European Commission, What is the role of the Data Protection Authority? https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-role-data-protection-authority_en accessed 27 March 2026.

¹⁵⁶ Data Protection Authority & you (n154).

¹⁵⁷ Bird & Bird, ‘ICO, CNIL, German and Spanish DPA Revised Cookies Guidelines: Convergence and Divergence’ (2021) < https://www.twobirds.com/en/insights/2019/global/ico-and-cnil-revised-cookies-guidelines-convergence-and-divergence?utm_source=chatgpt.com> accessed 27 March 2026.

¹⁵⁸ CNIL, Délibération n° 2020-092 du 17 septembre 2020 portant adoption d’une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs, République Française, < <https://www.cnil.fr/sites/cnil/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf>> accessed 24 May 2026.

is continuing to browse a website.¹⁵⁹ Instead, consent for the placement of trackers should be based on “clear affirmative action”, that could include for example clicking a checkbox to agree, as well as one to disagree¹⁶⁰ Data subjects should be conscious on the scope of the consent, purpose of the cookies as well as be able to take it back at any given moment.¹⁶¹ After the publication of the guidelines, CNIL has prescribed sanctions on organisations on non-compliance, including Google and Shein.¹⁶²

In 2024, as a result of the increased popularity of ‘consent or pay’ models, DPA’s from several countries, including German, Norway and Netherlands requested the EDPB to publish an opinion, later referred to as the Opinion 8/2024 concerning the issue.¹⁶³ The request was a result of growing concern regarding the fact that there was no uniform approach to consent or pay models within the EEA nor a common consensus among the data protection authorities on the acceptability of the model.¹⁶⁴ In addition to that, the request concerned whether data subjects are able to exercise real choice under the ‘consent or pay’ models, paying specific attention to “risk of deception, intimidation, coercion or significant negative consequences”.¹⁶⁵

2.4 EDPB interpretation of consent

The EDPB has published the following documents on consent pursuant to the GDPR: Guidelines 05/2020¹⁶⁶ and Opinion 08/2024.¹⁶⁷ While neither the

¹⁵⁹ CNIL, Cookies et autres traceurs : la CNIL publie des lignes directrices modificatives et sa recommandation (2020) <<https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/lignes-directrices-modificatives-et-recommandation>> accessed 24 May 2026.

¹⁶⁰ CNIL (n159).

¹⁶¹ Nafiye Yücedağ, Elif Beyza Akkanat Öztürk, Şehriban İpek Aşıkoğlu, ‘Cookies and other trackers, Pay or Consent Models in Europe: Already Outdated or an Overlooked Crisis in Freely Given Consent?’ Technology and Regulation, (2025) p 339.

¹⁶² CNIL: Cookie regulation: the CNIL is continuing the action plan initiated in 2019 and has imposed two fines on SHEIN and GOOGLE (2025)<<https://www.cnil.fr/en/cookie-regulation-cnil-continuing-action-plan-initiated-2019-and-has-imposed-two-fines-shein-and>> accessed 27 March 2026.

¹⁶³ Datatilsynet (n17).

¹⁶⁴ Datatilsynet (n17).

¹⁶⁵ Request, Section II (‘Background and reasoning of this request’), A. Legal framework regarding the fundamental concept of consent, p. 2

¹⁶⁶ Guideline 05/2020 (n51).

¹⁶⁷ Opinion 08/2024 (n28).

guideline nor the opinion constitutes a binding legal source, they do reinforce harmonious application of the GDPR within the European Economic Area.¹⁶⁸

Guidelines 05/2020 on Consent under Regulation 2016/679 is a document built upon its predecessor Article 29 Working Party Guidelines on Consent under Regulation 2016/679.¹⁶⁹ The purpose of the document is to analyse the concept of consent as defined under GDPR.¹⁷⁰ Meanwhile the document addresses the conditions of obtaining and demonstrating valid consent, it does not consider ‘consent or pay’ models as a part of its analyse. In line with its predecessor, the guideline examines what constitutes a freely given, specific, informed, and unambiguous consent under GDPR.¹⁷¹ Opinion 08/2024 on valid consent provides an assessment of consent or pay models implemented by large online platforms. The opinion concerns whether consent or pay models relating to behavioural advertising can be implemented by large online platforms in a way that constitutes a valid consent.¹⁷² The opinion of the EDPB follows the CJEU’s reasoning regarding the factors taken into account when assessing whether data subject’s consent can be required as valid.¹⁷³ The same criteria has also been used in Guidelines 05/2020.¹⁷⁴

Whereas the ruling established how the conditions of validity as set in Article 4(11) GDPR, especially the condition of freely given is to be interpreted, the EDPB explains this criterion by creating a guideline that further clarifies the ruling.¹⁷⁵ The CJEU considered that the data subjects could be offered an equivalent alternative, a fee to guarantee that there is an opportunity for the data subjects to freely refuse consenting to data processing.¹⁷⁶ The EDPB takes this view further by recommending third alternative that would not require a payment from data subjects. The central idea of the third alternative would be that it would not include behavioural advertising, which in turn

¹⁶⁸ Opinion 08/2024 (n28).

¹⁶⁹ Guidelines 05/2020 (n51), p4.

¹⁷⁰ Guidelines 05/2020 (n51), p 4.

¹⁷¹ Guidelines 05/2020 p 5.

¹⁷² Opinion 08/2024 (n28)

¹⁷³ Opinion 8/2024 (n28) para 70.

¹⁷⁴ Opinion 8/2024 (n28) para 70.

¹⁷⁵ Opinion 8/2024 (n28) para 67-140.

¹⁷⁶ Bundeskartellamt (n133) para 150.

would strengthen the validity of the consent by minimising the element of detriment.¹⁷⁷ It is clear from the wording of the opinion, that the EDPB takes the stance that a binary choice between accepting to processing or personal data or paying a fee cannot be regarded as valid consent pursuant to the GDPR.¹⁷⁸ Overall, the opinion aims to establish an EU-level guidance on ‘consent or pay’ models and harmonize the application of GDPR with regards to ‘consent or pay’ models implemented by online platforms.¹⁷⁹

As a whole, the EDPB opinion examines personal data from the viewpoint of fundamental rights, which is to be seen as a typical approach taken by data protection authorities.¹⁸⁰ The viewpoint, however, does not take into consideration¹⁸¹ the demand and supply structure of the online platforms, in terms of generating revenue from the business users and advertisers through the use of personal data.¹⁸²

¹⁷⁷ Opinion 8/2024 (n28) page 3.

¹⁷⁸ Opinion 8/2024 (n28) page 3

¹⁷⁹ Opinion 8/2024 (n28) page 7.

¹⁸⁰ De Moraes (n4),p 12.

¹⁸¹ De Moraes (n4),p 12.

¹⁸² Pinar Akman, A web of paradoxes: Empirical evidence on online platform users and implications for competition and regulation in digital markets (2022) Virginia law & business review, volume 16, (2022) number 2, P 223.

3 CONSENT IN ‘CONSENT OR PAY’ MODELS

3.1 Closer look at consent or pay models

The EDPB defines ‘consent or pay’ models as a regime where data subject is offered a choice by the controller in order to access an online service provided by that controller.¹⁸³ The central idea of the model is that the data subjects can choose between accessing the free version of the service and consenting to their data being processed for a specified purpose or pay an fee and access the version of the service that does not include data processing for the before-mentioned purpose.¹⁸⁴ The consent, given by the data subjects who do not want to pay for the service relates to being tracked and targeted for behavioural advertising. While the data subjects who decide to pay for the service are not targeted with behavioural advertising, they might still be tracked for other purposes.¹⁸⁵

Even though the focus of this chapter is on consent or pay models implemented by online platforms, other types of variations exist. For example, paywalls constitute a variation of consent or pay models.¹⁸⁶ Generally put, paywalls are systems that are able to generate revenue by adding a fee as a prerequisite for accessing a certain website.¹⁸⁷ Paywalls are most commonly used by online newspapers. They can be divided into two categories based on the level of limitations they pose for access. The categories are “hard” paywalls and “soft” paywalls.¹⁸⁸ With hard paywalls, used by online newspapers such

¹⁸³ Opinion 08/2024 (n28) p 9.

¹⁸⁴ Yücedağ (n 161).

¹⁸⁵ Opinion 08/2024 (n28) p 9.

¹⁸⁶ Noyb (n18)p 13.

¹⁸⁷ Panagiotis Papadopoulos, Peter Snyder, Dimitrios Athanasakis, Benjamin Livshits, keeping out the Masses: Understanding the Popularity and Implications of Internet Paywalls, In Proceedings of The Web Conference (2020)(WWW ’20), April 20–24, 2020,p1.

¹⁸⁸ Papadopoulos (187) p 3.

as the Financial Times, the readers are able to read a selected number of articles after which they are provided with the requirement to subscribe in order to keep reading.¹⁸⁹ Soft paywalls, used by online newspapers such as the Guardian and Helsingin Sanomat have both free and paywalled articles, which are only accessible for subscribers.¹⁹⁰

3.2 The oxymoron of consent within consent or pay models

The GDPR is influenced by the concept of “*informational self-determination*,”¹⁹¹ which was a term first introduced by a German constitutional ruling in 1983. It established individuals’ capability of making decisions regarding the use and disclosure of their personal data.¹⁹² The concept of informational self-determination is reflected in the GDPR in the form of consent. However, consent does not automatically result in such empowerment of data subjects, multiple as factors can have an effect on the capability of individuals in making decisions that have long term consequences.¹⁹³ The reliance of data subjects ability to make decisions regarding the processing of their personal data is at the core of consent or pay models implemented in online platforms.

However, are data subjects actually able to grasp what is it, that they are consenting to? In a study published in Virginia Law & Business Review in 2022, roughly 11 000 consumers from different countries were asked whether they know how Facebook can provide its service to users for no cost. The study revealed that majority of the respondents couldn’t come up with the correct answer to the question.¹⁹⁴ 23% of the respondents answered, “I don’t know”, whereas 26% of the respondents thought the data collected in sold to other companies. Only 42% of the respondents knew the correct answer to be that

¹⁸⁹ Noyb (n18)13.

¹⁹⁰ Noyb (n18)13.

¹⁹¹ Jakub Misek, Data protection as a performance-based regulation, Research handbook on EU Data protection law, Eleni Kosta, Ronald Leenes, Irene Kamara (2022), p51.

¹⁹² Bundesverfassungsgericht BrV 109/83, Judgment of 15 December 1983, Para 147

¹⁹³ The role of consent in an algorithmic society-its evolution, scope, failings and re-conceptualization, Bart Custers, (n 79)p 468.

¹⁹⁴ Akmant (n182) 248.

“advertisers pay the platform provider to show me ads when I use this particular service.”¹⁹⁵ Respondents were told that some platforms are free of cost because they are able to monetize personal data through personalised advertising.¹⁹⁶ Precisely 42% of the respondents answered that meanwhile they do not want to be targeted with ads, they also would not be willing to pay for the services either. Essentially 60% of the respondents were in the opinion that the arrangement benefits them more than the company.¹⁹⁷

As provided in Article 4(11)¹⁹⁸ and interpreted in *Orange Romania*¹⁹⁹, consent has to be based on sufficient amount of information.²⁰⁰ Article 12 of the GDPR provides that the information must be provided in a “clear and plain language”²⁰¹, pointing into the direction that data subjects should be informed in a way that they have a capacity of understanding. However, online platforms often have privacy notices that are characterised by lengthy texts that which are built upon complicated legal glossary,²⁰² which in turn does not encourage data subjects into reading the content of the privacy notice. As stipulated by various researchers²⁰³ the majority of data subjects do not have the habit of reading privacy notices.²⁰⁴ Regardless of whether data subjects would spend the time reading the privacy notice, it would still remain unclear whether they have actually understood what happens to the data processed.²⁰⁵

When you add the element of a payment to the equation, the legitimacy of the consent becomes even more questionable. According to a study conducted in Austria, over 70% of participants dismiss the idea that companies would be able to process their personal data while using an online platform, but nevertheless 88% of them would choose to consent when provided with the option

¹⁹⁵ Akmant (n182) p249.

¹⁹⁶ Akmant, (n182) p250.

¹⁹⁷ Akmant, (n182) p 251.

¹⁹⁸ GDPR (n1) Article 4(11).

¹⁹⁹ *Orange Romania* (n125).

²⁰⁰ Custers (n88), p 11.

²⁰¹ GDPR (n1) Article 12

²⁰² Custers (n88), p 11.

²⁰³ Custers (n88). p 9.

²⁰⁴ Solove (n15) p 1884,

²⁰⁵ Custers (n88), p 11.

of agreeing to being tracked or to pay a fee.²⁰⁶ In 2025, a report published by Noyb²⁰⁷, a non-governmental organisation focused enforcing data protection laws, stated that over 99% of users are choosing to consent to tracking instead of paying on German-speaking websites with only 1% of user choosing to not consent.²⁰⁸ These numbers indicate that most users are choosing to consent to data processing when faced with consent or pay walls, nevertheless of their actual preferences. When examining the causes leading into this kind of phenomenon, the factors can take several forms depending on the banner faced by the data subject. In general, the factors can include having consent as a prerequisite for using the website, decision fatigue, or even a hurry.²⁰⁹

3.3 The building blocks of freely given consent

As provided earlier, consent or pay models rely on data subjects' consent on processing of personal data. For consent to be considered legitimate, it has to be freely given.²¹⁰ The EDPB defines "freely given" as a real choice and control practised by data subjects.²¹¹ When analysing whether consent provided by a data subject in the 'consent or pay' model can be regarded as freely given, as stipulated in Article 4(11) GDPR, a criteria derived from the GDPR, interpreted by the CJEU in *Meta v Bundeskartellamt* and by the EDPB in its guidelines should be considered.²¹² To begin with, freely given consent should encompass genuine and free choice, where the data subject is able to refuse or withdraw consent without detriment.²¹³ As a second criterion, there

²⁰⁶ Dr Brigitte Naderer, Genuine Choices in Pay or Okay, Examining the role of the options consent, payment and advertisement in pay or okay models, "Consent or Pay" study report < https://noyb.eu/sites/default/files/2025-12/noyb_Con-sent_or%20Pay_Study_User_Choice.pdf > accessed 24 May 2026

²⁰⁷ Noyb, about us <<https://noyb.eu/en/about-us>> accessed 16 April 2026

²⁰⁸ Noyb (n18).

²⁰⁹ Nataliia Bielova, Laura Litvine, Anyisia Nguyen et al., The Effect of Design Patterns on (Present and Future) Cookie Consent Decisions, USENIX Security 2024 - 33rd USENIX Security Symposium, (2024), p 2815.

²¹⁰ Custers (n88) p 4.

²¹¹ Guidelines 5/2020 (n51) para 13.

²¹² Opinion 08/2024(n28) para 70.

²¹³ Bundeskartellamt (n133) para 143.

should not be an evident imbalance between the controller and the data subject as²¹⁴ consent cannot be regarded as freely given if a clear imbalance between the controller and data subject is evident.²¹⁵ Data subjects should also be able to consent separately to different data processing operations.²¹⁶ Finally, attention should be paid whether there is an element of conditionality, meaning that the consent of the data subject is a prerequisite for using the service, when the processing is not obligatory for the performance of the contract.²¹⁷ Whether an online platform is able to meet this criteria should be assessed in a case by case basis the purpose of the next chapter.

²¹⁴ Bundeskartellamt (n133) para 144.

²¹⁵ GDPR (n1) recital 43.

²¹⁶ Bundeskartellamt (n133) para 144.

²¹⁷ Bundeskartellamt (n133) para 145 and para 70, see also EDPB Opinion 08/2024, p 9.

4 CRITICAL ANALYSIS OF FREELY GIVEN CONSENT IN LARGE ONLINE PLATFORMS: CASE STUDY ON META PLATFORMS

This chapter examines ‘consent or pay’ models in the context of very large online platforms (VLOPs). The aim of the chapter is to create a case study that assesses whether the consent or pay model implemented by Meta Platforms is able to fulfil the requirement of freely given consent under Article 4(11) GDPR, reflecting it with factors including power imbalance, conditionality, granularity and detriment to the data subject. Meta Platforms, the owner of two significant social media platforms, Facebook, and Instagram as well as the owner of an instant messaging service WhatsApp and Messenger,²¹⁸ is chosen as the subject of the analysis, because it represents a well-known example of consent or pay model implemented in a very large online platform. It is also chosen as the focus this chapter, because of its dominant market position, evident from its designation as a gatekeeper under Digital Markets Act in 2023.²¹⁹ The delimitation of the analysis is the acknowledgement that the consent or pay model implemented by Meta Platforms does not embody every consent or pay model, but rather demonstrates whether consent or pay models implemented by very online platforms that have a dominant market position, with little to no competition are able to at all fulfil the requirements of freely given consent as it is understood within the EU legal framework outlined in the second chapter.

The online platforms examined in this chapter are Instagram and Facebook. Both Instagram and Facebook are structured under the same business model, implementing a very similar consent or pay model. The business model under

²¹⁸ Tuulia Karjalainen, ‘The battle of power: Enforcing data protection law against companies holding data power’, *Computer Law & Security review*, Volume 47, 105742 (November 2022).

²¹⁹ Summary of Commission Decision of 5 September 2023 relating to a decision pursuant to Article 3 of Regulation (EU) 2022/1925 (Digital Markets Act) C(2023).

which both Instagram and Facebook operate is grounded in personalized advertising which²²⁰ is defined for the purpose of this section as a form of advertising that is grounded in the observation of behaviour of a data subject.²²¹ The permission for personalized advertisement is provided by data subjects who accept the general terms when they create their profile on Facebook or Instagram for the very first time.²²² This is specifically stipulated in Meta’s annual report from 2024, which states that Meta Platforms generates the vast majority of its revenue from advertising conducted by marketers on Facebook and Instagram.²²³ As a result of this common ground the platforms are assessed together.

In 2023, Meta Platforms introduced a new business model for the region of the European Union, called consent or pay.²²⁴ This was a direct result of the *Bundeskartellamt*²²⁵ ruling that required Meta to change its legal base for behavioural advertising from “legitimate interest” to “consent” for the data subjects operating within EU, EEA and Switzerland.²²⁶ Following the implementation of the subscription-based consent or pay model, used by Meta has received a great deal of scrutiny in relation to its compliance with GDPR, DMA as well as consumer protection laws.²²⁷

4.1 The technicalities of the subscription-based model

As for 2026, both Instagram and Facebook implement a subscription based ‘consent or pay’ model, where data subjects are able to subscribe to a fee that allows them to use the service with no ads or continue using the service for free with ads.²²⁸ The price of the subscription varies from monthly payment

²²⁰ Bundeskartellamt (n133) para 27.

²²¹ A29WP Opinion 2/2010 (n21) p 4.

²²² Bundeskartellamt (n133) para 28.

²²³ Meta 2024 Annual report p 17.

²²⁴ De Moraes (n4) p2.

²²⁵ Bundeskartellamt (n133).

²²⁶ Meta Annual Report 2024, page 10.

²²⁷ D’Amico (n21), p 256.

²²⁸ Facebook help center, About subscription for no ads<<https://www.facebook.com/help/262038446684066>>accessed 24 May 2026.

of €5.99 to €7.99, depending on whether the subscription is conducted through website or app store.²²⁹ Another variable that affects the price is whether the data subject has more than one account linked to the same account center.²³⁰ Each account rises the price of monthly subscription by €5.²³¹ The price was changed to its current amount in 2024, when Meta decided to lower the value of subscription prices that had been set to €9.99 and €12.99.²³²

4.2 Assessment of consent obtained by Meta Platforms

As mentioned above in the previous chapter, the elements of freely given consent consists of genuine and free choice without detriment to the data subject in case of withdrawal,²³³ no clear imbalance between the data subject and the controller,²³⁴ ability to consent individually to each processing operation²³⁵ and not using consent as a prerequisite for the use of service when it's not obligatory for the performance of contract.²³⁶

4.2.1 Detriment to the data subject

When assessing whether Meta's 'consent or pay' model is able to provide data subjects with a valid consent within the meaning of Article 4(11) GDPR, in particular the requirement of freely given, the starting point is to assess what does the model implemented by Meta encompass. To everyone who subscribes, Meta promises an ads free experience where the personal information of the data subject is not used for advertising.²³⁷ Data subjects who do

²²⁹ Instagram Help Center, Subscription for no ads <<https://help.instagram.com/923021729404927>> accessed 3 April 2026.

²³⁰ Instagram Help Center (n229).

²³¹ Instagram Help Center (n229).

²³² Meta, 'Facebook and Instagram to Offer Subscription for no Ads in Europe' (November 12, 2024) <<https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/>> accessed 6 April 2026.

²³³ Bundeskartellamt (n133) para 143.

²³⁴ Bundeskartellamt (n133) para 144.

²³⁵ Bundeskartellamt (n133) para 144.

²³⁶ Bundeskartellamt (n133) para 145, 70, see also EPDB Opinion 08/2024, p 9.

²³⁷ Instagram (n229).

not want to subscribe to monthly payments can continue to use Meta's platforms free of charge with advertisement.²³⁸ In order to use the free version of the platform, Meta requires the data subject to consent to the following: Meta will continue to process personal data from data subjects user accounts for advertisement purposes as well as to continue on using cookies on Meta's products for personalized advertisement and to measure how they perform.²³⁹ However, due to the preliminary findings of the European Commission in 2024 regarding the compliance of the binary 'consent or pay model' with the Digital Markets Act, EDPB opinion 8/2024 and criticism from European consumer protection organisations, Meta also introduced a third option to its users in November 2024.²⁴⁰ The third option includes a less personalized advertisement option for the data subjects who are using the free version of the platform.²⁴¹

The first assessment is whether data subjects are able to refuse or withdraw consent without detriment pursuant to recital 42 GDPR.²⁴² The EDPB asserts that in a situation where data subjects do not give their consent to data processing nor pay the subscription fee requested by Meta, they will not be able to use the service at all.²⁴³ The EDPB elaborates that in a situation like this, there is a potential that data subjects will face a detriment, as depending on the service, the platform can serve as an important space for example of social interaction.²⁴⁴ Considering this from the viewpoint of Meta platforms, the detriment faced by the data subject is presumed to be related mostly to social sphere.

Alternatively, Noyb has pointed out that Meta's 'consent or pay' model requires different level of effort from the data subject, depending on whether

²³⁸ Instagram (n229).

²³⁹ Meta Platforms Inc, Instagram (mobile application, iOS version 350.0.2026)

²⁴⁰ Meta Platforms, Annual report on Form 10-k For the fiscal year ended December 31, 2024, (2024) p 10. < https://s21.q4cdn.com/399680738/files/doc_financials/2024/ar/Meta-12-31-2024-10K-ARS.pdf> 24 May 2026.

²⁴¹ Meta (n240) p 10.

²⁴² Guidelines 5/2020 (n51) para 46.

²⁴³ Opinion 08/2024 (n28) para 86.

²⁴⁴ Opinion 08/2024 (n28) para 87-88.

they agree to consent or refuse to consent.²⁴⁵ This is due to the fact that refusing consent takes more time, as data subjects have to either enter their bank details or pay through apple or google accounts.²⁴⁶ Consenting, on the other hand occurs by choosing the free version with ads on the first layer and then choosing between personalised and less personalised ads on the second layer.²⁴⁷ Considering the argument that refusing consent is more time consuming than consenting, it could be drawn that the data subject might experience detriment to some degree by choosing to pay for ads free version. The EDPB opinion also mentions downgrade of the performance of the service as a negative consequence that can be qualified as a detriment to the data subject.²⁴⁸ The less-personalized ads version comes with ad breaks that stop the user from browsing on the platform for a certain amount of time.²⁴⁹ It could be argued that this feature has a negative effect on the user experience in comparison to the version with personalised advertisement, which does not include obligatory ads breaks, which in turn could nudge users towards choosing personalised ads. The negative impact on users was also acknowledged by Meta itself in its annual report from 2024, describing less-personalised ads as a development which might have negative impacts on user growth and engagement.²⁵⁰ Another difference between the two free versions of the platform is related to professional accounts. The less personalised option does not let users to boost their posts on the platform,²⁵¹ meaning that users who have a professional account and are aiming to grow their brand through reaching a bigger audience might not be able to do it as effectively without choosing the personalised advertisement option.²⁵² These factors may have an effect on

²⁴⁵ Noyb (n150),p 7.

²⁴⁶ Noyb (n150),p 7.

²⁴⁷ Meta Platforms Inc, Instagram (mobile application, iOS version 350.0.2026).

²⁴⁸ Guidelines 05/2020 (n51) para 48.

²⁴⁹ Instagram Help Center, About less-personalized ads <https://help.instagram.com/2009526812842911/?helpref=related_articles> accessed 3 April 2026

²⁵⁰ Meta (n240).

²⁵¹ Meta business Help Center, Understand how certain ads choices limit your ability to advertise and monetize <https://www.facebook.com/business/help/1563729837497242?helpref=faq_content> accessed 3 April 2026.

²⁵² Instagram Help Center, Boost a post on Instagram <<https://help.instagram.com/2090822074310288>> accessed 3 April 2026.

whether users are choosing to use the free version of the platform with less personalised ads or with personalised ads.

When it comes to the pricing of the subscription, there is no definitive rules provided by the GDPR with regards to the pricing practises linked to ‘consent or pay’ models.²⁵³ Data protection authorities are able to only examine, if the price associated with the subscription is “reasonable.”²⁵⁴

4.2.2 Power imbalance between the controller and the data subject

In terms of imbalance of power between the data subject and the controller, as provided in recital 43 GDPR²⁵⁵, the emphasis is paid on Meta’s market dominance.²⁵⁶ Even though the power imbalances mentioned in the GDPR refer to public authorities, the EDPB has stated that imbalance of power does not only encompass public authorities or employers.²⁵⁷

The criterion is further assessed by the EDPB in its recent opinion, which provides that even if the controller cannot be regarded as having a market dominance, the imbalance between the controller and the data subject can come from the lack of alternatives data subjects have when it comes to services, including social media platforms aimed for content sharing.²⁵⁸ The EDPB pays an emphasis on services, which have been able to gather a significant amount of users by offering their services for free and then switching up and started applying pay or consent models. By being free, the service might have drawn in a lot of users that would have not joined if there was a fee from

²⁵³ Pay or consent, Status quo on the European Market, April 2024, p 12
<https://www.bvdw.org/wp-content/uploads/2023/10/PUR-Modelle-bvdw_20231004-en.pdf> accessed 6 April 2026.

²⁵⁴ Pay or consent (n253)p12- 13.

²⁵⁵ GDPR (n1)Recital 43.

²⁵⁶ Opinion 8/2024 (n28) para 100

²⁵⁷ Guidelines 5/2020 (n51) para 24.

²⁵⁸ Opinion 8/2024 (n28) Para 105

the start. These users might have depended on the service and now experience that there is not a free choice on whether to consent to processing or not.²⁵⁹

WhatsApp has introduced ads in 2025, which are based on limited information such as geographic information or data derived from other Meta accounts from different platforms.²⁶⁰ Although ads on WhatsApp are not based on users' consent in the same manner as they are on Facebook and Instagram, the update reflects the trend that Meta is able to access a significant amount of information from the users of its platforms within the Europe and as a result of this Meta has been able to build a notable amount of market power.²⁶¹ As several of the platforms owned by Meta have a significantly wide user base and also implement the same consent or pay model, data subjects might be left to feel that they do not have other options than to consent if they want to keep using the service. The wider user base of the platform in comparison to other options might make the user feel dependent on the platform and therefore the option of choosing another platform can be impractical.²⁶²

4.2.3 Conditionality

The criterion of conditionality originates from Article 7 GDPR.²⁶³ Article 29 Working Party highlighted the importance of Article 7(4) when assessing whether consent is freely given. It provided that tying consent together with accepting terms which are not necessary for the performance of the contract cannot constitute a freely given consent.²⁶⁴ The EDPB confirmed this view and proposed that consent can be freely given if access to service is not made dependent on data subjects consent.²⁶⁵ Conditionality was also analysed in *Meta v Bundeskartellamt* where the CJEU found that data subjects should be free to reject processing operations that are not necessary for the performance

²⁵⁹ Opinion 8/2024 (n28) para 109.

²⁶⁰ Helping You Find More Channels and Businesses on WhatsApp (2025) <https://about.fb.com/news/2025/06/helping-you-find-more-channels-businesses-on-whatsapp/> accessed 24 May 2026.

²⁶¹ About Facebook (n260).

²⁶² Opinion 8/2024 (n28) para 108

²⁶³ GDPR (n1) Article 7.

²⁶⁴ A29WP Guidelines (n83) p 8.

²⁶⁵ Guidelines 05/2020 (n51).

of the contract.²⁶⁶ With this regard the CJEU mentioned the option of appropriate fee.²⁶⁷

A scholarly article published in *Technology and Regulation* in 2024 argued that the access to service within the business model applied by Meta is dependent on the data subjects' consent for processing personal data that is not essential for its service, as advertising is not regarded as necessary for a service to be provided for the user.²⁶⁸ According to this assessment, Meta's business model would be contrary to Article 7(4) GDPR²⁶⁹, which emphasises that freely given consent cannot be conditional processing of personal data that is not necessary for the service.²⁷⁰

As mentioned earlier, Meta offers its users three options: to pay a fee or to consent to processing of personal data for behavioural advertising with the option of less personalised ads. The description of the less-personalized ads is the following: *"You'll have a different ad experience. You'll see a variety of products and brands through ads that are less related to your interests. You may see ad breaks. Less of your data will be used for ads"* While the option of personalized ads is described as *"Discover products and brands that are related to your interests and activity on Meta Company products. Your data will be used for ads"*²⁷¹ The information collected of the data subject for personalized advertisement consists of behaviour on the platform, including how the data subject engages with posts, the content viewed, the interaction with ads as well as information from the data subject's user profile given by the data subject themselves.²⁷² For less-personalized ads the information collected encompasses whether the data subject interacts with ads, profile and device information as well as the content viewed by the user.²⁷³

²⁶⁶ Bundeskartellamt (n133) para 150.

²⁶⁷ Opinion 08/2024 (n28) para 116.

²⁶⁸ D'Amico (n21) p258.

²⁶⁹ GDPR (n1) Article 7(4).

²⁷⁰ GDPR (n1) Article 7(4).

²⁷¹ Meta Platforms Inc, Instagram (mobile application, iOS version 350.0.2026).

²⁷² Instagram Help Center, Manage whether you see personalized or less-personalized ads <https://help.instagram.com/426488546963771/?helpref=related_articles> accessed 24 May 2026.

²⁷³ Instagram Help Center (n272).

The EDPB has previously stipulated that if the controller is able to provide the data subject with an opportunity to choose between data processing and alternative version that does not include processing of personal data, the service would not be regarded as conditional.²⁷⁴ The EDPB also further explained the point made by CJEU in *Bundeskartellamt* regarding “equivalent alternative”, by stating that if the controller is able to offer an equivalent version which is different from the original only in a way that it does not process personal data for behavioural advertising, it could be regarded as equivalent.²⁷⁵ The third option provided by Meta has distinctive differences (e.g. ad breaks) in comparison to the paid version of the service, making it less likely to be regarded as an equivalent alternative, as conceptualised by the EDPB.

4.2.4 Granularity

In accordance with the opinion of the EDPB, consent or pay models should provide data subjects with an opportunity to separately choose each of the data processing purposes they want to accept, meaning that purposes should not be offered as a batch.²⁷⁶ The EDPB pays an emphasis to challenges of granularity within large online platforms, however without taking a stance on whether Meta fulfils this criterion.²⁷⁷ However, by assessing the consent banner Instagram provides for data subject’s that are using the platform, it is quite evident that there is only the option to pay and not have personalised advertisement, not pay and have personalised advertisement or not pay and have less personalised advertisement. Data subjects are not provided with a genuine opportunity to select which data processing purposes they would like to give their consent to as the purposes are presented as bundled together. Nevertheless, personalised advertising is not the only purpose Meta processes personal data for as data is also processed for purposes such as analytics.²⁷⁸ To

²⁷⁴ EDPB Guidelines on consent, paragraph 37.

²⁷⁵ Opinion 8/2024 (n28), para 121.

²⁷⁶ Opinion 8/2024 (n28) para 139.

²⁷⁷ Opinion 8/2024 (n28) para 140.

²⁷⁸ Meta, What is the Privacy Policy and what does it cover? <https://www.facebook.com/privacy/policy> accessed 14 May 2026.

adhere with the requirements of Article 21 GDPR²⁷⁹ Meta provides data subjects with a possibility to object to the processing of personal data for certain purposes when the legal basis of the said processing is legitimate- or public interest.²⁸⁰ However, after the *Bundeskartellamt*²⁸¹ ruling held that legitimate interest pursuant to Article 6(1)(f) GDPR cannot be relied on as a legal base for personalised advertising²⁸² the legal basis within Meta Platforms was changed to consent.²⁸³ As a result of this shift data subjects actual ability to exercise of the right to object is a concern worth exploring further.

4.3 Deceptive design patterns in consent or pay models

The concept of dark patterns was first introduced by Harry Brignull, who defines the term as “deceptive patterns”, used for influencing data subjects’ decision making when they are visiting a website or using an app.²⁸⁴ Dark patterns are considered to contravene with the data protection principles set out in the GDPR, especially with the principle of fairness, that prohibits processing of data that is misleading to the data subject.²⁸⁵ The concept is highly related to consent or pay models in social media platforms, as a prerequisite of valid consent is that data subjects are not predisposed to deceptive design patterns when they are required to consent to data processing operations.²⁸⁶

²⁷⁹ GDPR (n1) Article 21.

²⁸⁰Information about objections and how you can object on Meta Products <<https://www.meta.com/en-gb/help/quest/126192406164229/?srsltid=Afm-BOoryTNXs4Wj0XUSaTaWjMuxyXdWsW68IdKvA-ZjmgEOS6Ddw2Dn3>> accessed 14 May 2026.

²⁸¹ Bundeskartellamt (n133).

²⁸² noyb – European Center for Digital Rights, 'Cease and Desist: Training of Meta AI in the EU' (14 May 2025) p 2 https://noyb.eu/sites/default/files/2025-05/noyb_cease%20and%20desist%20letter_Meta%20AI_pub.pdf accessed 14 May 2026.

²⁸³ Meta (n240).

²⁸⁴Harry Brignull, 'Deceptive Patterns (aka Dark Patterns)' (Deceptive Design) <https://www.deceptive.design/> accessed 17 May 2026.

²⁸⁵ EDPB Guidelines 4/20219 on Article 25 Data Protection by Design and by Default (20 October 2020) p. 16; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en. accessed 24.5.2026.

²⁸⁶ Opinion 8/2024 (n28).

In a broad sense, dark patterns are able to manipulate data subjects into taking a certain action that is a result of the usage of different techniques, such as ambiguous or misleading language used by a website.²⁸⁷ The objective of the design might be to direct the data subject into making a choice that is beneficial for the company, such as buying a product²⁸⁸ and therefore amplifying the sales of the company.²⁸⁹ With regard to gaining access to users personal data dark patterns can be used as an *attention diversions* or as a *last minute consent*.²⁹⁰ An attention diversion can be used on a cookie wall placed on a website. The colour of the consent button can function as an attention diversion by having a colour that distinguishes it clearly from the background (green) meanwhile the decline button is purposely coloured in a way (grey or white) that makes it stand out less. Last minute consent can be displayed as a confirmation for consent that is being asked when the data subject is already in a rush, for example finishing an order.²⁹¹ Another example of dark patterns used in consent setting is placing “agree” and “reject” buttons on different layers of the cookie banner.²⁹² Placing “agree” button on the first layer with an “option” button next to it makes users more likely to press the agree button, as according to Noyb only around 2 % of data subjects pay a visit to the second layer.²⁹³ Throughout the many methods, dark patterns are able to negatively affects data subjects’ capability to protect their personal data.²⁹⁴ In 2018, Norwegian Consumer Council Forbrukerrådet issued a report detailing

²⁸⁷Harry Brignull, 'Trick Wording' (Deceptive Design) <https://www.deceptive.design/types/trick-wording> accessed 17 May 2026.

²⁸⁸ Finnish Competition and Consumer Authority, 'Dark Patterns' (KKV) <https://www.kkv.fi/en/consumer-affairs/scams/dark-patterns/> accessed 17 May 2026.

²⁸⁹ Maximilian Maier, Rikard Harr, DARK DESIGN PATTERNS: AN END-USER PERSPECTIVE, 2020 Volume 16(2), August 2020, 170–199, ISSN: 1795-6889, Human Technology, University of Jyväskylä.

²⁹⁰ CNIL, Shaping Choices in the Digital World, 2019 P 28. https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf accessed 17 May 2026.

²⁹¹ CNIL, Shaping Choices in the Digital World, P 27

²⁹² European Center for Digital Rights, Consent Banner Report: Overview of EU and National Guidelines on Dark Patterns, p 10 https://noyb.eu/sites/default/files/2024-07/noyb_Cookie_Report_2024.pdf accessed 18 May 2026.

²⁹³ Noyb, Consent banner report, overview of EU and national guidelines on dark patterns Page 10.

²⁹⁴ CNIL (n290).

the use of dark patterns in big technology companies²⁹⁵ such as Facebook, claiming that Facebook uses techniques such as pre-selected default settings for privacy, hidden privacy intrusive default settings and opt-out designs.²⁹⁶ In 2022, the EDPB published guidelines dealing with dark patterns on social media platforms²⁹⁷, indicating a growing concern towards the phenomenon, emphasising the role of social media platforms. Prior to 2022, EDPB has discussed dark patterns indirectly in relation to valid consent and controller requirements under GDPR.²⁹⁸ Opinion 8/2024 assesses dark patterns in the context of consent or pay models in social media platforms, insisting large online platforms to not include deceptive design patterns in their designs asking for data subject's consent.²⁹⁹

4.4 Complementary GDPR principles

As emphasised by the EDPB, acquiring consent from data subject is not enough alone and controllers have to also take into consideration other central GDPR principles, including data minimisation, purpose limitation, fairness, data protection by design and default and accountability.³⁰⁰

Regardless of whether the data subject has given her consent to the processing of personal data, the data collected should not exceed what is necessary for the specified purpose or be unfair.³⁰¹ The objective of the purpose limitation principle is to protect data subjects by placing limits on the way or purposes for which data is being used.³⁰²

²⁹⁵ Forbrukerrådet (Norwegian Consumer Council), *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy* (2018).

²⁹⁶ Forbrukerrådet, *Deceptive by design, how tech companies use dark patterns to discourage us from exercising our rights to privacy* (2018), p 13-17.

²⁹⁷ EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them (14 February 2023).

²⁹⁸ See guidelines 05/2020 on consent under regulation 2016/679.

²⁹⁹ Opinion 8/2024 (n28) para 182.

³⁰⁰ Opinion 8/2024 (n28) para 183.

³⁰¹ Guidelines (n51)05/2020 para 5.

³⁰² Ronald Leenes, Eleni Kosta, Irene Kamara, 'Introduction to Research Handbook on EU data protection law', p 7.

Under the data minimisation principle, personal data processed should be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected”³⁰³ Among with the principles of proportionality, necessity and purpose limitation, the EDPB has emphasised the role of data minimisation principle with regards to data processing. When it comes to behavioural advertising, controllers operating large online platforms often aim to collect personal data of data subjects as extensively as possible, merging data from different sources together, within and outside the platform.³⁰⁴ Instagram and Facebook implement a business model, which operates by using the information of data subjects to generate specific profiles about them. The information used for the profiles is a combination of personal data provided by the data subject themselves when they sign up for the service for the very first time as well as information that has been collected outside of the platform.³⁰⁵ The information collected from various sources is then used for advertisement, which is shown for the data subjects that are using the free version of the service.³⁰⁶

The principle of data minimisation with regard to personalized advertisement was analysed in a ruling *Schrems v Meta*³⁰⁷, where the CJEU stipulated that the data minimisation principle prohibits controllers from collecting and processing data subjects’ personal data without limitations for personalised advertisement.³⁰⁸ The judgment also placed a limit on the usage of sensitive data for advertisement purposes.³⁰⁹ To supplement the ruling, opinion of the EDPB provides that controllers should consider whether the processing of personal data for specific purposes could be conducted with less intrusive means or through processing fewer personal data.³¹⁰

³⁰³ GDPR (n1) Article 5(1)(c).

³⁰⁴ Opinion 8/2024 (n28) para 59.

³⁰⁵ Bundeskartellamt (n133) para 27.

³⁰⁶ Bundeskartellamt (n133) para 28.

³⁰⁷ C-446/21 Maximilian Schrems v Meta Platforms Ireland Ltd ECLI:EU:C:2024:834.

³⁰⁸ Shrems (n307) para 65.

³⁰⁹ Shrems (n307) para 84(2)

³¹⁰ Opinion 8/2024 (n28) para 58.

As of 2026, Facebooks privacy policy states that the data collected includes activity across the Meta products, information about the connections and contacts of the data subject, device information, purchases off- the platform, information on which apps are used by the data subject as well as data received from third parties outside Meta products.³¹¹ It remains unclear whether Meta’s business model is able to satisfy the requirement of data minimisation under GDPR. The EDPB has assessed that tracking that combines information on data subjects from multiple sources is likely to not be compatible with the principle of data minimisation in comparison to a mechanism where data subjects are able to choose which data is used.³¹²

4.5 Counter argument: freedom to conduct business

As ‘consent or pay’ models are most often based on business models that generate their revenue from online advertising that is grounded in collecting behavioural data of data subjects³¹³, one could argue that personal data is used in a way as a commodity traded for free use of service. However, the discussion on whether personal data can be used as a commodity in this manner has been discussed in various scholarly articles and publications of European data protection authorities. Multiple arguments reinforce the view that while personal data cannot be regarded as tradeable commodity.

One argument is that because the protection of personal data is a fundamental right enriched in Article 8 of the Charter³¹⁴; it has an inalienable nature. The inalienable nature of fundamental rights guarantees that the right to personal data protection cannot be deprived, transferred, or lost.³¹⁵ To develop this argument further the EDPB argued in its guideline published in 2019 that as the GDPR aims to empower data subjects with authority over their own infor-

³¹¹ Meta (n278).

³¹² Opinion 8/2024 (n28) para 59.

³¹³ Opinion 8/2024 (n28) para 15.

³¹⁴ Charter of Fundamental rights (n32) Article 8

³¹⁵ Bart Custers, Gianclaudio Malgieri, Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data, *Computer Law & Security Review*, Volume 45, 105683 (2022).

mation and regardless of whether the data subject would consent to processing operations, the fundamental right to data protection cannot be traded away in this manner.³¹⁶ In a more recent publication from 2024, the EDPB examined the tradeable commodity argument from the perspective of the binary nature of consent or pay models that offer an appropriate fee as an option opposed to processing operations. The EDPB reflected the concept of “appropriate fee” discussed in *Meta Platforms Inc and Others v Bundeskartellamt*, stipulating that the fee should not develop the fundamental right to data protection in a way that it becomes a paid right, only protecting those who can afford it.³¹⁷

Approaching the phenomenon of consent or pay models within large online platforms prompts the question of whether platforms such as Instagram or Facebook should be free of charge to begin with. Freedom to conduct business is a fundamental right enriched in EU Charter of Fundamental Rights.³¹⁸ Meta describes its business model based on advertisement as a “cornerstone of an inclusive internet where everyone can access online services and content for free.”³¹⁹ and personalised advertisement as a benefit that provides data subjects with an opportunity to find new products they might like based on the information gathered of them.³²⁰ The way in which Meta frames its business model pays an emphasis on how data subjects benefit from the processing of their personal data, leaving out the details concerning the reduced privacy.

As of May 2025, Meta started using public information, including the name, pictures and actions of data subjects for developing generative AI models as well as AI Meta based on legitimate interest. The information concerning data

³¹⁶ EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (8 October 2019) para 54.

³¹⁷ Opinion 08/2024 (n28) para 132.

³¹⁸ Charter of Fundamental Rights (n32) Article 16.

³¹⁹ Meta, Facebook and Instagram to Offer Subscription for No Ads in Europe <<https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/>> accessed 14 May 2026.

³²⁰ Meta, Facebook and Instagram to Offer Subscription for No Ads in Europe <<https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/>> accessed 14 May 2026.

subjects is used for the improvement of AI as a default setting and users who do not want to consent have to actively choose to opt-out throughout objection. Nevertheless, information on data subjects who choose to send an objection might still be used for AI development if personal information on them is made publicly available on them by someone else on the platform, such as a photo shared by someone else.³²¹ Prior to May 2025, the use of personal data for AI development had already been identified as a concern by national data protection authorities, the EDPB and other organisations such as Noyb. It could be conducted that this practise reflects a broader approach applied by Meta when it comes to protecting the fundamental rights of data subjects. It suggests that Meta may not consider the privacy-related aspects beforehand but rather adjusts its approach to privacy protection when faced with criticism or enforce measures from the European regulators. Whether this is an issue resulting from different approaches to privacy between the EU and the U.S or whether there is another reason behind this remains contested.

³²¹ Meta Platforms Inc, Instagram (mobile application, iOS version 350.0.2026).

5 CONCLUSION

The purpose of this thesis was to examine, to what extent is the ‘consent or pay’ model implemented by large online platforms compatible with the requirement of freely given consent under article 4(11) GDPR. The answer to this research question was conducted through an analysis of three sub-questions.

The first sub-question essentially asked, how is valid consent understood under the GDPR and how has the concept been interpreted and developed through CJEU case law and EDPB recommendations. The research provided that valid, in particular freely given consent is understood as “freely given, specific, informed and unambiguous indication of the data subject’s wishes.”³²² Consent should consist of active behaviour of the data subject. There should be no detriment to the data subject in case of refusal of consent or withdrawal, ³²³ the data subject should hold sufficient amount of information, ³²⁴ consent should be asked separately to each data processing operation³²⁵ and no conditionality where consent is used as an exchange for the service by forcing data subjects’ consent.³²⁶

In order to answer the second sub-question, which asked, to what extent are data subjects able to exercise a valid, in particular freely given consent, when faced with a consent or pay model implemented in large online platforms and what are the conditions these platforms have to meet in order to fulfil the requirement of freely given consent? The research assessed data subjects’ ability to make independent decisions that reflect their actual will to consent to data processing activities by reflecting into studies conducted by various researchers. The research showed that when it comes to consent or pay models implemented by online platforms, data subjects are likely to consent to

³²² GDPR (n1) Article 4.

³²³ Opinion 8/2024 (n28) para 70.

³²⁴ Orange Romania (n125).

³²⁵ Opinion 8/2024 (n28) para 7.

³²⁶ Opinion 8/2024 (n28) para 70.

data processing when faced with consent or pay models, nevertheless of their actual preferences regarding data processing.

The research of the third sub-question, to what extent does the consent or pay model implemented by Meta platforms fulfil the requirement of freely given consent under Article 4(11) GDPR was conducted by examining Meta's consent or pay model against the criteria of detriment, no power imbalance, conditionality and granularity, based on the conditions of freely given consent, provided by EDPB in its Opinion 8/2024.³²⁷ The answer to the research question states that, while the consent or pay model, applied by Meta is not able to fully satisfy the requirements of freely given consent, this does not mean that any online platform is not able to satisfy them. In terms of Meta's consent or pay model, the most significant obstacles are related to Meta's dominant market position and the lack of competition, the ability of the third alternative (less-personalised ads) to comprise equivalent alternative, bundled consent, compliance with the data minimisation principle as right to object under GDPR.

The answer to the main research question is the following: Whether online platforms are able to provide data subjects with a freely given consent as it is understood in Article 4(11) GDPR, is a case-by-case analysis that should be conducted to the platform, reflecting it to the criteria provided in Opinion 8/2024.³²⁸ Large online platforms with dominant market position, little to no competition and binary consent or pay model are likely to have harder time passing this criteria whereas online platforms that are able to provide data subjects with a real equivalent alternative might be able to provide data subjects with a freely given consent.

³²⁷ Opinion 8/2024 (n28).

³²⁸ Opinion 8/2024 (n28) para 71.

6 Bibliography

6.1 EU LEGISLATION

Charter of Fundamental Rights of the European Union [2000] OJ C364/1

Consolidated version of the Treaty on European Union [2016] OJ C202/1

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, repealing Directive 95/46/EC (General Data Protection Regulation) [2016] L 119/1

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, OJ L 281

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) (2002) OJ L 201

6.2 SCHOLARLY ARTICLES

Akmant P, A web of paradoxes: Empirical evidence on online platform users and implications for competition and regulation in digital markets (2022) Virginia law & business review, volume 16, (2022) number 2.

Bielova N, Litvine L, Nguyen A et al., The Effect of Design Patterns on (Present and Future) Cookie Consent Decisions, USENIX Security 2024 - 33rd USENIX Security Symposium (August 2024).

Bolognini L, Covello L, Fiordalisi G, ‘Admissibility of the ‘pay or consent’ model: between digital economic revolution and data protection modernisation’ (2024)< <https://zenodo.org/records/10848258> >accessed 30 March 2026

Custers B, Malgieri G, Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data, Computer Law & Security Review, Volume 45, July 2022, 105683

D’Amico A, Pelekis D, Santos C, Duivenvoorde B, Meta’s Pay-or-Okay Model, An analysis under EU Data Protection, Consumer and Competition Law, Technology and Regulation (2024).

- De Moraes P, Claudet P, 'Pay or consent to have your data used- the complex intersection between the DMA and data protection rules, International review of law, computers & technology (2026) University of East Anglia
- Harry Brignull, 'Deceptive Patterns (aka Dark Patterns)' (Deceptive Design) <https://www.deceptive.design/> accessed 17 May 2026.
- Janeček V, Malgieri G 'Commerce in Data and the Dynamically Limited Alienability Rule', Cambridge University press (2019) .
- Karjalainen T, 'The battle of power: Enforcing data protection law against companies holding data power', Computer Law & Security review, Volume 47, 105742 (November 2022).
- Maier M, Harr R, DARK DESIGN PATTERNS: AN END-USER PERSPECTIVE, 2020 Volume 16(2), August 2020, 170–199, ISSN: 1795-6889, Human Technology, University of Jyväskylä.
- Misek J, Data protection as a performance-based regulation, Research handbook on EU Data protection law, Eleni Kosta, Ronald Leenes, Irene Kamara (2022).
- Morimoto M. (2021). Privacy concerns about personalized advertising across multiple social media platforms in Japan: the relationship with information control and persuasion knowledge. *International Journal of Advertising*, 40(3).
- Müller-Tribbensee T, Miller K, Skiera B, 'Paying for Privacy: 'Paying for Privacy: Pay-or-Tracking Walls' (HEC Paris research paper No. MKG-2024-1514)
- Nam S, Kwon Y, 'Is pay-or-consent for privacy justifiable? Evidence from different users' privacy attitudes toward behavioral data collection in South Korea' School of Business and Technology Management, Telecommunications policy (2024).
- Nettesheim M, EU Data Protection Law and Pay-or-Consent Business Models, University of Tübingen Law School (2024) p 2.
<<https://dx.doi.org/10.2139/ssrn.4768419>> accessed 24 May 2026
- Papadopoulos P, Snyder P, Athanasakis D, Livshits B, keeping out the Masses: Understanding the Popularity and Implications of Internet Paywalls, In Proceedings of The Web Conference (2020)(WWW '20), April 20–24, 2020.
- Solove DJ, Murky consent: an approach to the fictions of consent in privacy law, Harvard Law Review 1880 (2013)

Smiths J, ‘What is legal doctrine? on the aims and methods of legal-dogmatic research, Maastricht European private law institute working paper no. 2015/06.

Schermer B Custers B, prof. Simone van der Hof, The Crisis of Consent, How Stronger Legal Protection may lead to Weaker Consent in Data Protection, Leiden University Faculty of Law, Ethics and Information Technology (2014)

Tauqeer A, An integrated approach to GDPR-compliant data sharing employing consent, contracts, and licenses, Data & Knowledge Engineering, volume 162 (2026)

Utz C, Degeling M, Fahl S, Schaub F, Holz T. 2019. (Un)informed Consent: Studying GDPR Consent Notices in the Field. (2019) ACM SIGSAC Conference on Computer and Communications Security, <<https://arxiv.org/pdf/1909.02638>> accessed 14.5.2026.

Yücedağ N, Beyza E, Öztürk A, Aşıkoğlu S, ‘Cookies and other trackers, Pay or Consent Models in Europe: Already Outdated or an Overlooked Crisis in Freely Given Consent?’ Technology and Regulation. (2025).

Van de Waerdt P, Meta v Bundeskartellamt: Something Old, Something New, European Papers, Vol 8, 2023, No 3, PP. 1077-1103.

6.3 POLICY PAPERS

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, ‘Guidelines 8/2020 on the targeting of social media users’ (13 April 2021).

EDPB Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms.

Article 29 data protection working party, Opinion 15/2011 on the definition of consent (13 July 2011) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> accessed 24 May 2026

EDPB Guidelines 05/2020 on consent under Regulation 2016/679 (4 May 2020) < https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 24 May 2026

EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, (7 July 2021), p 3 <https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf> accessed 24 May 2026

Article 29 Working Party Guidelines on consent under Regulation 2016/679 (28 November 2017)

EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (8 October 2019) para 54.

EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them (14 February 2023).

EDPB Guidelines 4/20219 on Article 25 Data Protection by Design and by Default (20 October 2020) p. 16; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en. accessed 24.5.2026.

6.4 ONLINE SOURCES

Datatilsynet ‘Request for an EDPB opinion on “consent or pay” (Datatilsynet) <<https://www.datatilsynet.no/en/news/aktuelle-nyheter-2024/request-for-an-edpb-opinion-on-consent-or-pay/>> accessed 25 February 2026.

Noyb, Pay or Okay Report (2025) <https://noyb.eu/sites/default/files/2025-07/Pay_or_Okay_Report_2025_web.pdf> accessed 24 May 2026

European Commission, Commission sends preliminary findings to Meta over its “Pay or Consent” model for breach of the Digital Markets Act (2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3582> accessed 24 May 2026

What is GDPR, The EU’s new data protection law?’ <<https://gdpr.eu/what-is-gdpr/>> accessed 3 March 2026

Forbrukerrådet, DECEIVED BY DESIGN, How tech companies use dark patterns to discourage us from exercising our rights to privacy (2018)<<https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf> < accessed 18 April 2026

An Official Website of the European Union, Data protection authority & you https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-authority-and-you_en accessed 27 March 2026.

European Commission, What is the role of the Data Protection Authority? <https://commission.europa.eu/law/law-topic/data-protection/rules-business->

and-organisations/enforcement-and-sanctions/enforcement/what-role-data-protection-authority_en accessed 27 March 2026

Bird&Bird, 'ICO, CNIL, German and Spanish DPA Revised Cookies Guidelines: Convergence and Divergence' (2021) <https://www.twobirds.com/en/insights/2019/global/ico-and-cnil-revised-cookies-guidelines-convergence-and-divergence?utm_source=chatgpt.com> accessed 27 March 2026

CNIL, Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs, République Française, < <https://www.cnil.fr/sites/cnil/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf>> accessed 24 May 2026

CNIL, Cookies et autres traceurs : la CNIL publie des lignes directrices modificatives et sa recommandation (2020) <<https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/lignes-directrices-modificatives-et-recommandation>> accessed 24 May 2026

CNIL: Cookie regulation: the CNIL is continuing the action plan initiated in 2019 and has imposed two fines on SHEIN and GOOGLE (2025)<<https://www.cnil.fr/en/cookie-regulation-cnil-continuing-action-plan-initiated-2019-and-has-imposed-two-fines-shein-and>> accessed 27 March 2026

Bundeskartellamt official website <<https://www.bundeskartellamt.de/EN/Bundeskartellamt/AboutUs/aboutus.html#:~:text=The%20Bundeskartellamt%20is%20the%20most,to%20protect%20competition%20in%20Germany>>Accessed

Noyb, 'Complaint under article 77(1) GDPR' (November 2023) p 9. <<https://noyb.eu/sites/default/files/2023-11/Complaint%20-%20Meta%20Pay%20or%20Okay%20-%20REDACTED.pdf>> accessed 24 May 2026

Dr Brigitte Naderer, Genuine Choices in Pay or Okay, Examining the role of the options consent, payment and advertisement in pay or okay models, "Consent or Pay" study report < https://noyb.eu/sites/default/files/2025-12/noyb_Consent_or%20Pay_Study_User_Choice.pdf > accessed 24 May 2026

Noyb, about us <<https://noyb.eu/en/about-us>> accessed 16 April 2026

Facebook help center, About subscription for no ads<<https://www.facebook.com/help/262038446684066>>accessed 24 May 2026

Instagram Help Center, Subscription for no ads <<https://help.instagram.com/923021729404927>>accessed 3 April 2026

Meta, 'Facebook and Instagram to Offer Subscription for no Ads in Europe' (November 12, 2024) <<https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/>> accessed 6 April 2026.

Meta Platforms, Annual report on Form 10-k For the fiscal year ended December 31, 2024, (2024) p 10. <https://s21.q4cdn.com/399680738/files/doc_financials/2024/ar/Meta-12-31-2024-10K-ARS.pdf> 24 May 2026.

Instagram Help Center, About less-personalized ads <https://help.instagram.com/2009526812842911/?helpref=related_articles> accessed 3 April 2026

Instagram Help Center, Boost a post on Instagram <<https://help.instagram.com/2090822074310288>> accessed 3 April 2026.

Meta business Help Center, Understand how certain ads choices limit your ability to advertise and monetize <https://www.facebook.com/business/help/1563729837497242?helpref=faq_content> accessed 3 April 2026.

Pay or consent, Status quo on the European Market, April 2024, p 12 <https://www.bvdw.org/wp-content/uploads/2023/10/PUR-Modelle-bvdw_20231004-en.pdf> accessed 6 April 2026.

Helping You Find More Channels and Businesses on WhatsApp (2025) <https://about.fb.com/news/2025/06/helping-you-find-more-channels-businesses-on-whatsapp/> accessed 24 May 2026.

Instagram Help Center, Manage whether you see personalized or less-personalized ads <https://help.instagram.com/426488546963771/?helpref=related_articles> accessed 24 May 2026.

What is the Privacy Policy and what does it cover? <https://www.facebook.com/privacy/policy> accessed 14 May 2026.

Information about objections and how you can object on Meta Products <<https://www.meta.com/en-gb/help/quest/126192406164229/?srsltid=AfmBOoryTNXs4Wj0XUSaTaWjMuxyXdWsW68IdKvA-ZjmgEOS6Ddw2Dn3>> accessed 14 May 2026.

Meta, Facebook and Instagram to Offer Subscription for No Ads in Europe <<https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/>> accessed 14 May 2026.

noyb – European Center for Digital Rights, 'Cease and Desist: Training of Meta AI in the EU' (14 May 2025)p 2 https://noyb.eu/sites/default/files/2025-05/noyb_cease%20and%20desist%20letter_Meta%20AI_pub.pdf accessed 14 May 2026.

Information about objections and how you can object on Meta Products <<https://www.meta.com/en-gb/help/quest/126192406164229/?srsltid=AfmBOoryTNXs4Wj0XUSaTaWjMuxyXdWsW68IdKvA-ZjmgEOS6Ddw2Dn3>> accessed 14 May 2026.

Harry Brignull, 'Trick Wording' (Deceptive Design) <https://www.deceptive.design/types/trick-wording> accessed 17 May 2026

Finnish Competition and Consumer Authority, 'Dark Patterns' (KKV) <https://www.kkv.fi/en/consumer-affairs/scams/dark-patterns/> accessed 17 May 2026.

European Center for Digital Rights, Consent Banner Report: Overview of EU and National Guidelines on Dark Patterns,p 10 https://noyb.eu/sites/default/files/2024-07/noyb_Cookie_Report_2024.pdf accessed 18 May 2026.

6.5 BOOKS

Bullock E, Valid Consent, The routledge handbook of the ethics of consent (2018).

Custers B, Fosch-Villaronga E, Vander Hof S, Schermer B, Sears AM, Tamo-Larrieux A, The role of consent in an algorithmic society-its evolution, scope, failings, and re-conceptualization, Research Handbook on EU data protection law 2021

Kelleher D, Karen Murray, EU Data protection law, Bloomsbury (2018)

Kuner C, Bygrave LA, Docksey C, The EU General Data Protection Regulation (GDPR) A commentary, Oxford University press (2020)

Rosemary J, Guide to the General Data Protection Regulation, A companion to Data Protection kawa bd Practise (4th edition) (2017).

6.6 TABLE OF CASES

Case C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH ECLI:EU:C:2019:801

Case-201/14 Bara and Others ECLI:EU:C:2015:638

Case-291/12 Michael Schwartz v Stadt Bochum ECLI:EU:C:2013:670

Case-212/13 František Ryneš V Úřad pro ochranu osobních údajů,
ECLI:EU:C:2014:2428

Case-524/06 Huber, ECLI:EU:C:2008:724

Case-131/12 Costeja Gonzalez v Google Spain and Google,
ECLI:EU:C:2014:317

Case-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di
Lecce V Salvatore Manni, ECLI:EU:C:2017:197

Case-61/19, Orange România SA V Autoritatea Națională de Supraveghere
a Prelucrării Datelor cu Caracter Personal (ANSPDCP)
ECLI:EU:C:2020:901.

Case-61/19, Orange România SA V Autoritatea Națională de Supraveghere
a Prelucrării Datelor cu Caracter Personal (ANSPDCP) Opinion of Advo-
cate general, ECLI:EU:C:2020:158

Case C-252/21 Facebook Deutschland GmbH v Bundeskartellamt,
ECLI:EU:C:2023:537

Case C-446/21 Maximilian Schrems v Meta Platforms Ireland Ltd
ECLI:EU:C:2024:834

6.7 OTHER SOURCES

Bundeskartellamt case summary, Facebook, Exploitative business terms
pursuant to Section 19(1) GWB for inadequate data processing, case Sum-
mary (February 2019,) B6-22/16, p 7.

Bundesverfassungsgericht BrV 109/83, Judgment of 15 December 1983,
Para 147

Forbrukerrådet (Norwegian Consumer Council), Deceived by Design: How
Tech Companies Use Dark Patterns to Discourage Us from Exercising Our
Rights to Privacy (2018).

Summary of Commission Decision of 5 September 2023 relating to a deci-
sion pursuant to Article 3 of Regulation (EU) 2022/1925 (Digital Markets
Act) C(2023)